PROTECTING FOAA ONLINE

WITH ENCRYPTION TECHNOLOGIES

Protecting FOAA Online with Encryption Technologies
Year of publication: 2018

Written by Zothan Mawii
Edited by Rajen Varada and Gulshan Banas
Cover and Layout Design by Shaifali Chikermane and Vimal Pawar

Published by: Digital Empowerment Foundation
House No. 44, 3rd Floor,
Kalu Sarai, New Delhi-110016

To read this publication online, visit www.defindia.org/publication-2

PROTECTING FOAA ONLINE WITH ENCRYPTION TECHNOLOGIES

ACKNOWLEDGEMENT

This research paper would not have been possible without the support of the APC IMPACT, under which this project was conceptualised and conducted. We would also like to acknowledge the grassroots activists in Odisha whose responses to our interviews gave us insight into the state of affairs on the ground.

INTRODUCTION

Information and communication technologies (ICTs) have grown in leaps and bounds in recent years. The subsequent explosion of Internet enabled digital technologies has widened the scope of communication and information sharing to unprecedented heights. The last two decades have seen the proliferation of social networking sites and communication platforms from—chat rooms on AOL and Usenet to platforms like MySpace, Facebook, and messaging apps like WhatsApp, iMessage, and Viber. The affordances of ICTs and the Internet have enabled the creation of online communities based on shared interests, transcending traditional boundaries of space and time. With 60 per cent of the world online and the growing ubiquity of mobile devices the popularity of digital communications platforms is only set to grow.

However, as much as contemporary digital technologies offer users avenues for self-expression and the ability to form associations and communities, they are open to exploitation and misuse by governments, criminals, corporate interests, and fraudsters. Additionally, these apps expose users to myriad privacy and security issues. The interests of users need to be protected from data mining tactics, online censorship, Internet shutdowns, and any action that prevents individuals from exercising their fundamental human rights.

High on this list are the right to privacy, the right to freedom of expression, and the right to freedom of peaceful association and assembly as enshrined in the

Advances in communication technologies have become a double edged sword. While ICTs free users from the barriers of time and geography, they also leave users vulnerable to surveillance and violations of privacy. Encryption is one way to protect users against such dangers.

UN Declaration of Human Rights, several regional human rights mechanisms, national constitutions, and by regional multi-stakeholder groups. These rights are at the core of a free and democratic society and should be upheld especially with regard to the changing context in which human interactions are carried out. ICTs offer new avenues where these rights can be exercised. The globalised nature of information, communication, and economic systems in the digital age means that interactions online have become just as crucial as physical interactions when conducting economic and social transactions. The growing legitimacy of technologically mediated communications has come hand in hand with the growing sophistication of surveillance and tracking tools and increasing concerns for the protection and privacy of one's data. Advances in the field of ICTs have been a double edged sword—digital technologies have had a positive impact on many, creating unforeseen opportunities and allowing previously excluded groups into the mainstream. At the same time, digital tools are opening users to risks like the infringement of privacy, surveillance by the State and private interests, threats from hackers and fraudsters, and economic and social exclusion for those that lack access. Encryption technologies which are the current iteration of cryptographic practises that have been used for thousands of years protect user data. However, States are increasingly turning away from their responsibilities of protecting citizens and attempting to curb the use of encryption technologies. Encryption is essential to protecting personal information and data from prying eyes and has a direct bearing on users' ability to practice their fundamental human rights.

Encryption technologies ensure that users' communications are kept secure, upholding their right to privacy and allowing users' to exercise their freedom of expression by allowing them to opine freely, without fear of repercussion and monitoring by external forces. Social protest movements of the past few years like the Occupy movements, the Arab Spring, the Umbrella Revolution, and the Jan Lokpal movement have demonstrated the efficacy of using digital platforms to mobilise and organise protests and movements. These movements were mobilised primarily on public platforms like Facebook and Twitter, with the exception of the Umbrella Revolution which was mobilised on WhatsApp messaging groups. Activists and participants of these social movements need to be assured that they will be protected against surveillance tactics from security agencies. Therefore encryption becomes essential to protecting the right to peaceful assembly and association (FoAA). It should be noted that exercising FoAA hinges directly on the right to freedom of expression and the right to privacy. Since social networking sites and digital technologies have become the preferred modes of organising associations and assemblies, whether for their convenience or wide reach, users' data and their personal communications must be protected.

> Since social media are fast becoming one of the preferred modes of organising social protests and social movement for their convenience and ability to reach large audiences, protecting user data with encryption technologies has become essential to protecting human rights online.

This paper will explore the use of encryption technologies in the Indian context and the hurdles to popularising such technologies. Drawing from examples in other countries, it will compare India's current encryption policy with best practices in other countries. This paper will recommend ways in which secure communication applications can and should be utilised by Indian activists and human rights defenders drawing examples from their use in other countries. Research for this paper faced many limitations. Prime among them being that awareness of encryption technologies is limited. Those who currently use encryption technologies work in sensitive areas and getting on-ground examples has been a hurdle. Media reports of social movements in India hardly feature the use of encrypted technologies so the instances taken as examples has centred on those that have featured heavily on social media.

OBJECTIVES

This research paper seeks to emphasise the necessity of private and secure communications as a condition for the effective exercise of FoAA. Private and secure communications can be ensured by encryption technologies making the call for encryption crucial.

Drawing on legal frameworks on privacy, encryption and the right to FoAA as posited by the United Nations, the constitutions of other countries and the Indian constitution, this research paper will present the best practices in relation to ensuring users' privacy and the areas in which India's laws are lacking.

This paper will explore encryption standards used on three messaging apps – Signal, Telegram, and Firechat – and investigate how these apps were used by activists during protest movements. The level of privacy each app offers and their role in the enabling of FoAA will be the main focus of study.

Drawing upon case studies of social movements in India in recent years, this paper will point out how existing encrypted technologies could have been used and leveraged in these scenarios.

RESEARCH METHODOLOGY

Research for this paper was conducted using a multiple method approach.

Desk Review: Encryption laws and privacy issues pertinent to India were explored and compared with best practices from other countries. A comparison of the different secure communications applications has been made to compare different features and their use in different situations.

Media monitoring: Examples of the use of encrypted technologies in social movements around the world were monitored to demonstrate how encrypted technologies can protect activists and human rights defenders.

Interviews: Interviews were conducted with activists who work in rural India to gauge their level of knowledge and the hurdles they face when using secure communications.

STATE OF PRIVACY AND DATA PROTECTION IN INDIA

Prior to the landmark ruling by the nine judge bench on August 24, 2017, stating unequivocally that privacy is a fundamental right, the right to privacy as protected by the Constitution of India was an unsatisfactory one. Article 21 which protects the right to life and liberty was seen to incorporate the right to privacy. Article 19(1)(a) provides the right to freedom of speech and expression, while Article 22 protects an individual from unreasonable arrests, and Article 25 protects an individual's right to practise a profession or religion of his choice. Article 300-A protects an individual's right to property.

The Supreme Court of India's declaration that privacy is a fundamental right has crucial implications on data protection and information privacy. This has a come at a time when mobile and Internet use is rising steadily and data mining by private entities and government alike is becoming more commonplace.

Although these articles do not explicitly spell out the individual's right to privacy, these articles have been interpreted as giving rise to a limited right to privacy. However these interpretations are subject to a number of limitations, prime among them being the protection of the nation's sovereignty, superior countervailing purposes, or a state interest that needs to be served (Privacy International, 2017).

Although the Supreme Court of India recognised the fundamental right to privacy in a number of cases, the nature of the limitations to privacy as stated above were highly over reaching. However after the nine judge bench ruling, the right to privacy and civil liberties has been given a new lease of life. Although the right to privacy is not absolute, it is currently a robust one with the many contours of the right to personal privacy and, crucially to the case at hand, information privacy clearly laid out. Justice Nariman cited from the International Principles on the Application of Human Rights to Communications Surveillance in his opinion reinforcing the right to privacy and its importance to other rights like the freedom of speech and information, and freedom of association. (pg, 40 of his opinion, pg 390)

The social structure in India is based on community and not individuality, and this argument has been used a number of times to attack the need for more stringent privacy laws in the country. While it is true that most vernacular languages do not have a word for privacy and families have traditionally lived together in joint families, with household responsibilities being shared along gender lines and each family member having set duties and roles. A joint family structure does not allow for much deviation from one's responsibilities or the luxury of isolated actions. However, the ruling shatters the myth that the right to privacy is an elitist concern. In India, the joint family structure is breaking down in many urban areas due to the demands of the neo-liberal workforce. Western cultural practices are creeping into daily life for a number of reasons—corporate bodies setting up regional offices and bringing in their international work culture, returning students from different foreign countries setting up businesses by emulating western best practices, and the embrace of western pop culture ushered in by digital technologies. There is growing awareness regarding the need for privacy in personal and professional spaces on all fronts.

Privacy in the digital age is a major concern as the number of mobile and internet users grows exponentially in the country. An Internet and Mobile Association of India (IAMAI) report "Mobile Internet in India in 2016" shows that the number of mobile internet users in India was set to reach 420 million by June 2017. Penetration of mobile internet in urban India was 51 per cent while in rural India it was 16 per cent. According to the global compendium of digital stats compiled by We are Social and Hootsuite, India has 462 million internet users, with 35 per cent penetration. Mobile devices accounted for 79 per cent of web traffic in India till January 2017. With its sizable population, mobile and internet users in India is only set to rise. The still largely unconnected rural areas and women users are the next big potential for growth. Only 28 per cent of women own mobile phones according to a report by GSMA. While these numbers show promise for a connected India and a target market for device makers and service providers, the developmental needs of the country still fall short. India ranked 131 on the 2017 Human Development Index, behind all the BRICS nations.

The Internet has become an enabler of rights especially with respect to freedom of expression. India's ranking on global indices for freedom and development are quite low and need to be improved in order to offer all sections of the population a fair chance. Providing access to Internet infrastructure, digital literacy and security online could improve the situation.

The Heritage Foundation's 2017 Index of Economic Freedom ranked India 143 behind Pakistan and Bhutan. The index found India to be "mostly unfree" and "development uneven." India still has a long way to go in terms of development and providing equal and fair opportunities to all sections of the population. Large sections of the population are still unconnected with no means of access to the internet due to the lack of infrastructure.

The internet has become an enabler of rights. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue in his 2011 report stated that access to the internet should be a basic human right. In the current cultural political atmosphere, the internet has become a source of news, an avenue for education, political and social participation, and economic self-determination.

The Digital India project aims to effectively deliver services to citizens through digital tools. However, these must be considered in light of the country's record on democratic process and freedom. India ranked 32 on the Economist Intelligence Unit's Democracy Index 2016 and was labelled a flawed democracy with a political culture worse than some Sub Saharan countries with authoritarian regimes. It ranked 136 on the World Press Freedom Index in 2017 behind the United Arab Emirates, Burma and Palestine. In light of these evaluations, privacy and data protection policies in India become especially pertinent to protect citizens and human rights defenders against overarching measures from the State.

The strong argument for greater privacy protection is being made in light of the current government's push to interlink Aadhaar (biometric enabled universal ID database) to social schemes, accessing utilities, and banking activities. It is the poorer sections of society who require Aadhaar to avail of benefits which are vital for their survival. Although Aadhaar is being touted as a "pro poor" initiative, it could very easily be used to target the most vulnerable sections of the Indian population. It is crucial that their privacy is protected.

Data mining by apps and services and surveillance by States pose a threat to all users of the Internet. The need for greater privacy protection and security online is being championed in India although still limited to urban, educated circles.

Digital natives, those who have grown up with and not known a world without Internet and digital technologies, who now make up a sizeable portion of the urban class are contributing to the awareness regarding the need for stringent privacy and data protection laws. It is not enough for India to adopt existing privacy laws borrowed from the laws of other lands. Instead, laws must be framed keeping in mind the socio-cultural-economic context of India, the majority of the population for whom these concepts are still alien, and the rapidity with which technologies change. Digital technologies, be it fitness apps, social media platforms, e-commerce sites, and digital wallets have rendered surveillance and monitoring activities that were once in the purview of elite intelligence agencies run of the mill and accessible to most technology companies. Governing bodies must take cognisance of these issues.

For the last few years, the phrase "data is the new oil," has been thrown around by everyone from corporate bodies, government agencies, and venture capitalists. The digital technologies that run modern life are a treasure trove of data – data that can be leveraged into profit. Data mining is the practise of sorting through large data sets to gather new information. This has become possible due to the collection of large amounts of data by search engines, social media platforms, e-commerce websites, webpages, etc. The information collected by these applications is embedded in metadata. A treasure trove of usable data, metadata contains information like when a website is accessed, the amount of time spent on it, links clicked, IP address, etc. Algorithms are then used to analyse this data and gather information on user behaviour to better target advertising at them or increase their dependence on certain services. Big data can be used to manipulate user patterns and in some cases may even give users undue disadvantages. For example, data collected from a user's fitness application recording the owner's heart rate, exercise patterns, underlying health issues etc., if handed over to insurance companies could mean that a slightly unhealthy person could be charged a higher premium. The practise of data mining needs to be investigated so that regulations are put in place to protect users' privacy from corporate interests and government surveillance.

With the rampant increase in data mining practices by businesses and governments, it is imperative that users have control over the data that is collected from them through their everyday actions. Data protection and privacy are inextricably linked.

India does not yet have a data protection law. Currently, some section of the IT Act can be used to protect against data breaches and cyber attacks

In India, the Information Technology Act of 2000 defines data, and civil and criminal liability in the event of breach of data protection and the violation of confidentiality and protection. Section 2 (1)(o) of the act defines data as the "[R]epresentation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;"

Section 43 defines the penalty in the case of breach or damage to computers or computer systems. These include accessing data on computer without prior permission, introducing viruses to computer systems, damaging computer networks, and causing disruption or denying access to computer systems and networks among others. Section 66E sets out parameters for the violation of privacy with specific reference to private images and their circulation without permission.

“Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.”

Section 66 of the IT Act makes provisions to protect citizens against hate speech, cyber bullying, blackmail, revenge porn, the distribution of private communications, and child pornography. This section is one of the stronger parts of the Act and has been invoked numerous times in cases since it came into being.

Section 67C sets out the parameters for data retention and its protection. “Preservation and retention of information by intermediaries.–(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe. (2) any intermediary who intentionally or knowingly contravenes the provisions of subsection (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.” However, Section 69 of the IT Act sets out guidelines that allow the government to monitor and collect information for reasons of national security, to block public access to information to preserve national security.

The IT Act of 2000 has its strong points but also lacks when it comes to protecting certain fundamental rights of citizens. There are provisions in the law that give the state the authority to censor content and monitor its citizens. The implications of this on encryption and laws protecting data and privacy will be discussed below. The concept of privacy in India is an emerging one in public discourse and, if laws are to be written in to protect citizens’ right to privacy, law makers must take into account current arguments encompassing digital technologies. Encryption is vital to protecting privacy and mechanisms to protect users must be put into place to ensure the right to privacy and consequently the freedom of association and assembly.

ENCRYPTION

Cryptography is the practise of securing messages from third parties. Cryptography has been used for thousands of years with one of the easiest and earliest examples being Caesar's cipher. In a Caesar's cipher, letters are substituted by a number of positions down the alphabet. The receiver requires this key to decipher the message. Cryptography became more complex at the turn of the century during World War 1 followed by the advent of computers in World War 2. As devices and mathematical formulations got more sophisticated, so did encryption. In its current iteration, complex mathematical rules inform cryptographic practise, making it completely agnostic. Current encryption practise is an intersection of mathematics, computer science, electrical engineering and communication science. Long used by government and militaries to facilitate secret communications, its use has become widespread due to the proliferation of personal computers and digital technologies.

> Encryption transforms messages or data into unreadable forms in transit so that they can be deciphered only by the true recipient of the message/data. It is no more confined to military and covert operations but is now available on most digital devices with varying levels of security.

The rapid spread of information and communication technologies (ICT) and the ubiquity of mobile devices have rendered it a complete necessity. Contemporary approaches to secure and private communications rely on encryption, derived from ancient cryptographic principles. David Kaye, the UN Special Rapporteur on promotion and protection of the right to freedom of opinion expression, in his report on anonymity and encryption on digital technologies, defined encryption as the "process of converting messages information, or data into a form unreadable by anyone except the intended recipient". Encryption was previously used to protect military operations but now has become available and necessary for all users of digital technologies. The information age we are living in has transformed the way we conduct social and economic interactions, leading us to produce tonnes of data through the adoption of digital lifestyles. Digital technologies that dictate modern everyday life like banking apps, e-commerce websites, and social media operate by collecting user data, most times sensitive data, and leveraging this data to deliver its services. The ever-growing popularity of Internet-enabled telecommunication apps, like WhatsApp, used by over 200 million people in India alone (Singh, 2017), has made it imperative that provisions made to ensure users' privacy and confidentiality are protected.

End-to-end encryption is vital to protect the content of emails, images, web browsers, hard disks, and messages sent over apps. This entails scrambling the original message with a 'key' which is then deciphered by the receiver with a secret key. Scrambling the text can have countless permutations thus disallowing even modern computers to crack it. This ensures that data is not intercepted while in transit. This same process can be used to encrypt data that has already reached its destination, for example, data stored in devices and hard disks. In most messaging applications including WhatsApp, Facebook Secret Messenger (Facebook's encrypted messaging service which needs to be switched on by users), Signal, and Gmail, a property called perfect forward secrecy is used to add more protection. A random key is generated for each session without using a deterministic algorithm. So even if hackers get hold of a particular encryption key, they will not be able to decrypt all messages. This ensures that past communications are not compromised if the keys get compromised at a later date. Encryption protects the content of data that is sent, but does not by default protect metadata that carries information like the Internet Protocol (IP) address, timestamps of messages sent and received, and location coordinates. Metadata is a vital pool of information and should be treated as such. Currently, most for-profit messaging apps do not include metadata encryption leaving it vulnerable to law enforcement agencies, private players, and hackers.

In 2001, the US National Institute of Standards and Technology established the Advanced Encryption

Standard (AES) and is now adopted worldwide. AES uses a symmetric-key algorithm, which means that the same key is used by both the sender and receiver to encrypt and decrypt the message. AES operates on a block size of 128-bits and a key size of 128, 192 or 256-bits. The key size determines the number of transformation rounds the plaintext goes through to be converted into ciphertext. The higher the key size, the more secure the protection. 256-bit end-to-end encryption has become the standard for secure banking and communication platforms.

Corporate bodies are left to decide whether or not they choose to adopt these encryption standards. Apple and Research in Motion (RIM) have been exalted for strong encryption standards on their products. Apple famously refused to let the FBI access encrypted data fearing it would create precedent for future loopholes in the San Bernardino shooting case. RIM, the makers of Blackberry went back and forth with the Indian government on leaving a security key in escrow. Most governments however, issue recommendations to organisations stating directives to follow to protect personal data. The European Union (EU) has been particularly stringent on this. In 2012, the EU proposed extensive changes to its Data Protection Directive (Directive 95/46/EC) which seeks to protect citizens' data during collection, processing and storage. The General Data Protection Regulation (GPDR) was adopted by the European Parliament and European Council in April 2016 and will become enforceable in May 2018. GPDR expands on existing requirements for collecting, storing, and sharing personal data and requires explicit consent from the subject. With strict rules in places, regarding data breaches and data privacy, organisations dealing with data of European citizens are likely to turn to stronger encryption standards to protect data and minimise their risks.

In India, the conversation around encryption and protecting personal data is a nascent one. Citizens of the country have been quick to adopt digital technologies but educated use of devices and social networking sites continues to be lacking. 77 per cent of urban users and 92 per cent of rural users consider mobiles to be the primary device to access the internet. For many first time users of the internet, social media sites like Facebook and WhatsApp are gateways to the wider internet. Content shared on these sites, no doubt, can be of a questionable nature due to the participatory nature of the internet. It takes a discerning digitally literate user to differentiate genuine content from fake news and hoaxes and this is getting increasingly hard with the proliferation of unverified viral content and the polarisation of political thought and opinion. For many first time users of digital devices, concepts like data mining, secure communications, data leaks and compromised security are not of high concern. Nor is there much awareness about them. There is a clear lack of awareness of security standards on digital devices among lay users. The proliferation of cheap devices with low security has people scrambling for them so they can gain access to and reap the benefits of the digital age. Issues like data protection and privacy are hard concepts to sell to Indian users who have little knowledge of the mechanisms of social media platforms, how the digital economy works or the ramifications of being digital citizens. Public discourse around privacy and security has largely been portrayed as elitist concerns. However this is starting to change in light of the government's push towards Digital India and concerns over the security of UIDAI's Aadhaar project and the recent Right to Privacy judgement. The government's attempt at introducing a Draft data protection bill was widely critiqued and is at the time of writing this paper, asking the public to submit recommendations. Public discourse needs to re-frame the privacy and security debate as a necessity for all, especially the poorer sections of society who are especially vulnerable to surveillance tactics and whose access to their basic necessities is at risk. While India seems to be galloping into the digital age with tremendous push from the government, it has lagged behind in adopting strong data protection policies. In

Digital literacy and nuanced consumption of digital media is lacking in a large number of mobile and Internet users in India, especially in rural parts. There is a lack of awareness of security issues and protections against and the proliferation of cheap devices with little security features is exacerbating the security threats that Indian users face.

order to protect the human rights of its citizens it needs to adopt policies that are tailor made to the unique Indian socio-cultural-economic context, addressing the concerns of different strata.

India is yet to implement a data protection law and existing provisions do not mention encryption standards. However the Reserve Bank of India does recommend encryption standards to be used for financial transactions.

ENCRYPTION LAWS

Governments the world over are moving towards enforcing restrictions on using encryption because the same technologies that protect user privacy prevent law enforcement authorities from conducting surveillance on potential criminals and terrorists. The potential of users to "go dark" thanks to encryption technologies has led both democratic governments and repressive States to curb the use of encryption.

India's stance on encryption is a contradictory one. The government advises strong encryption levels be followed in banking, e-commerce, and in firms that handle sensitive data. However, it places limitations on the strength of encryption to 40-bits under a licensing agreement with telecommunications firms. Section 84(a) of the IT Act, 2000, allows the government to "prescribe the modes and methods for encryption", although it does not specifically set encryption levels. Companies operating encryption levels higher than permissible are obliged to release encryption keys to escrow by the government as in the case of Blackberry's parent company Research in Motion.

In 2008, the government of India released a draft policy framework to regulate encryption in India which was met with widespread criticism. The draft policy proposed that encryption algorithms and keys would be set by the government, users could be obliged to hand over encrypted data along with encryption software to the government, and all encrypted messages, be it messages or e-mails, would have to be stored in plain text for 90 days. The government withdrew the heavily panned draft proposal and has not released an alternative yet. India does not have strong data protection laws nor does it have laws that explicitly protect the right to privacy, leaving citizens open to surveillance and monitoring by security agencies and hackers alike.

India may fare well on global indices for press freedom and freedom of expression when compared to its South Asian neighbours, but in the absence of laws to protect data and privacy, and the ambiguity of legal frameworks surrounding encryption, citizens are left quite exposed to cybercrimes and curbs on their human rights. The freedom to peaceful assembly and association whether online or offline depends on free and open expression and the assurance that compromised communications will not be used to self-implicate citizens. India should observe the best practices followed by other countries and adapt them to its current situation.

For example, Germany is known for its fierce protection of citizens' privacy and their data. It is no surprise that the German federal government encourages and recommends the use of encryption technology. There are provisions in the German cryptographic policy, drafted in 1999, that seek to provide confidence in the security of encryption rather than restrict the use of it (Schulz & Hoboken, 2016). The constitution protects citizens' right to secure information technology systems that will ensure their privacy and confidentiality. Germany also puts the onus of protecting user data on corporate bodies with high penalties for breach of use. However, in light of recent radical terrorist activities sweeping across Europe, Germany has passed controversial laws expanding surveillance of encrypted messages via popular messaging apps like WhatsApp and Skype (Phys.org, 2017). The law allows German investigators to insert spyware into the devices of users to access data in encrypted messages. Experts in the technology industry have reiterated time and again that backdoors cannot be created for one specific group, and that the insertion of any such provision puts the entire system at risk. Similar moves are being debated in countries across Europe. The United Kingdom passed the highly criticised Snoopers' Charter or Investigatory Powers Act 2016 last year. The new surveillance law requires web and phone companies to store all users' browsing data for 12 months and give law enforcement officials unprecedented access to the data. Critics have stated that this law will embolden authoritarian regimes and it may be used to justify their own severe surveillance laws. These laws dilute citizens' right to privacy and put them at risk of racial profiling.

Brazil's Marco Civil, the first of its kind when it was approved in 2014, protects citizens' rights online based on the civil rights that citizens enjoy. It also includes provisions for net neutrality. The legislations covers the ways in which the Brazilian legal system will deal with particular issues related to Internet use (Medeiros & Bygrave, 2015). The bill lists multiple fundamental rights that need to be interpreted with respect to Internet use. There are provisions in the bill that inform the collection, use, storage, treatment, and protection of personal data. Marco Civil has provisions to protect personal data and although it shies from explicitly stating the right to encryption, it does make provisions to protect the secrecy of users' communications. India could emulate Brazil's example by creating such a bill that explicitly states the protection of its citizens online. However, in a rather contradictory move, the Brazilian government has passed four orders banning Whatsapp in the past several months over its parent company's, Facebook, refusal to hand over protected data to Brazilian authorities to aid in a criminal investigation.

Brazil's Marco Civil protects citizens' Internet rights. The first of its kind, it is a comprehensive law that regulates and and protects citizens' personal data and access to the Internet.

The debate on encryption in Asia is a varied one, covering position on either side of the spectrum. The Great Firewall of China, put in place by the Communist Party of China (CPC) to suppress dissenting voices is a case of extreme monitoring by the state where all data that flows through the Chinese cyberspace is accessible to authorities and closely monitored. Because China disallows most western technology companies to operate in the country, home-grown versions like Weibo for Twitter and search engine Baidu are available for citizens to use. Encryption technologies can be used in China by foreign investment enterprises and Sino-foreign ventures after obtaining the required permits and following set protocols. China's cyber security laws leave little space for anonymity, requiring real name registration to use messaging apps and other services, and surveillance capabilities and data localisation built into most applications. These laws have serious impact on human rights and affect citizen's right to privacy, their freedom of expression since dissent is swiftly extinguished, and FoAA whether it be online or offline is under constant and close scrutiny and any situation the CPC deems untoward is quickly penalised.

The political and financial system present in a country is an indicator of its stance on encryption. China with its authoritarian government has strict rules against encryption with small allowances for foreign companies. Singapore, on the other hand places little restrictions on encryption technologies that can be used in the country, motivated by financial interests.

In contrast, the financial hub of Singapore has little restrictions on encryption technology. Motivated by financial interests and encouraging international businesses to thrive, authorities place little restriction on encryption technologies that can be imported and used in the country. Data protection laws in the country direct organisations to protect personal data using reasonably available security arrangements (Field Fisher Waterhouse, 2013). However, in Singapore, laws make provisions to protect financial interests and are not entirely invested in human rights. Opposition to the ruling party expressed online or in any media outlet is quickly extinguished because of the close ties between government and private press holdings. It is a common, if little known, practise to deny Internet access to bloggers and activists who use the Internet in ways that is not sanctioned by the ruling party (Shanthi Kalathil, 2003). Secure communications and data protection is encouraged by the government to protect financial interests and uphold the island nation's global reputation as a financial powerhouse. It is not rooted in protecting citizens' basic rights but rather encouraged to placate international financial players and their activities which have a direct bearing on Singapore's economy.

Communication is vital to the formation of assemblies and association, and today, online spaces are legitimate spaces to form these assemblies and associations. Secure communication, free from prying eyes whether it be law enforcement or corporate interests, is crucial for the practise of FoAA. The participatory nature of the social media enables participation in numbers that was not possible before, overcoming mitigating circumstances like location and time. Online communities and protest movements are not exclusively relegated to the realm of messaging apps and social media but are, in most cases, used to galvanise offline participation and physical action. Being able to express oneself without fear of surveillance and repercussion is crucial to the formation of online groups and communities. Online spaces double up as assemblies and associations in themselves and sites where traditional associations and assemblies can be organised.

SECURE COMMUNICATION TOOLS AND APPLICATIONS

There is a need to increase awareness of the importance of privacy and the promotion of protected communication and secure data. Below are some of the popular encrypted apps with examples of their user base in other countries. Indian activists and human rights defenders could do well to take examples and promote the use of such platforms.

Signal

Signal is an end-to-end encrypted messaging application for Android and iOS platforms developed by Open Whisper Systems in 2014. Since its initial release, the app has established itself as one of the more secure options available in the market. The app uses Curve 25519, AES-256, and HMAC-SHA 256 to encrypt messages and data and the keys used to encrypt data are stored on the device itself and not on external servers, so that even Open Whisper Systems does not have access to data. The use of AES-256 ensures that perfect forward secrecy is maintained and messages remain protected from future hacks. What sets the app apart from other secure messaging apps is that minimum metadata is collected by the app's developers, and subsequently deleted from its servers as soon as the message is delivered. Although technically when used on an iPhone, Apple's push notification feature can collect metadata. A passcode on the device will encrypt data that has already been received on the device, thereby protecting it from those trying to access messages and content remotely through the Cloud.

Signal is an open source secure communication app that is highly regarded within the tech and security community.

The app has a number of features that make it favourite of activists and privacy advocates, such as:

- Disappearing messages
- Safety number – a 60 digit number to verify privacy with a specific contact. Users need to compare the number or scan the QR code in order to verify each other's identities
- A verification code once the app is installed
- Encrypted voice and video calls
- Signal periodically sends truncated cryptographically hashed phone numbers for contact discovery without names or phone numbers on its servers. This lets users discover if their contacts are also using the app.

Open Whisper Systems has made the code for Signal freely and openly available on Github so that it can be scrutinised by experts and changes made according to needs. The app has been endorsed by whistleblower Edward Snowden and a number of well-known technologists. The company, based in San Francisco, is a non-profit and operates on donations from funders and grants from a number of foundations. WhatsApp, owned by parent company Facebook, enabled end-to-end encryption using Open Whispers System's algorithm last year. However, Facebook still has access to and controls metadata collected through the use of the app, giving corporate interests and security agencies access to data that could inadvertently reveal copious amounts of information. So while messages remain free from prying eyes, metadata can still be used to surveil and monitor.

Signal has become the messaging app of choice for a number of activists, high-level journalists, security personnel, and those handling sensitive information. Malkia Cyril, of Oakland based Center for Media Justice says that Black Lives Matter (BLM) activists have been using Signal since 2014 to organise BLM actions, in light of FBI surveillance over the movement (Smiley, 2017). In the USA, non-profit organisations like Planned Parenthood, Race Forward, and Women Action and Media are switching to Signal to communicate for fear of surveillance and DDOS attacks from political opponents after the election of Donald Trump as president. Even Hillary Clinton's campaign was rumoured to have switched to communicating via Signal after internal emails were leaked to the press. The app has been banned in Egypt and in June 2016, the Supreme Court rejected RTI activist Sudhir Yadav's plea to ban Signal and similar apps in India in the interest of national security.

Contemporary grassroots movements, whether it be the Arab Spring, Occupy Wall Street, Nuit Debout, the Umbrella Revolution or Black Lives Matter, share a common pattern—social media is used to mobilise participants and amplify the reach, followed by the occupation of a physical space. Although most of these movements have used the public reach of Twitter and Facebook to spread their message, it becomes imperative for core organisers and activists to have a space to communicate securely without fear of surveillance and persecution from security officials. Whether it be organising different actions through messaging apps, and cloaking identities to avoid arrest, activists and civil society organisations require secure communication technologies to exercise their right to FoAA both online or offline. Signal offers Black Lives Matter and civil organisations with the technological support it requires to carry out its activities. The preoccupation with encryption is slowly trickling down to the masses as news of widespread data collection and security breaches become public knowledge. Signal founder, Moxie Marlinspike's aim to make encryption commonplace and a default for all is a step in the right direction towards upholding human rights values and separating the human condition from corporate gains and state surveillance.

Telegram

Telegram is widely used by activists all over the world and has been used in a number of social protest and movements. It has been criticised by security officials as it is believed that criminals and terrorists use the app.

Telegram is a messaging application with end-to-end encryption, developed by the Durov brothers, Nikolai and Pavel. Nikolai provides technological support while Pavel contributes financial and ideological support. The app uses a custom designed encryption protocol called MTProto which is based on 256-bit symmetric AES encryption, RSA 2408 encryption, and Diffie-Hellman key exchange. The app can be used on Android, iOS, Windows Phone, Ubuntu Touch devices and on desktops as well. The client-side code is open source although the company does delay releasing some parts of its code. The server-side code is closed and proprietary. Telegram was one of the more popular secret messaging apps before critics pointed out the flaws in using a custom encryption code that do not follow industry norms and have not gone through the rigorous testing that the common encryption codes have gone through. Telegram is free to use and the website promises that it will remain so, and ads will not be displayed on the app.

The app allows users to send messages on a secret chat. Messages sent on secret chat have end-to-end encryption enabled and messages on secret chat self-destruct when either party tries to forward them. Users can also set self-destruct timers to messages sent on the app. These messages can only be accessed on the device of origin or reception. Regular messages (not secret chats) are transmitted through a cloud-based storage, allowing users to access their account from multiple devices. Users can send texts, documents, PDF files, and images upto 1.5 gigabytes in size. Messages can be sent to groups of up to 5000 and messages can be edited or deleted by either party (sender or recipient) up to 48 hours after the message has been sent. The app also allows users to make encrypted voice calls. The app can be made more secure by using a passcode for the app, thereby denying users access to the app even if the device gets stolen. Telegram, on its website, states that its multi data centre infrastructure and encryption technology ensures security. However, it has been pointed out that jailbroken and rooted access devices are susceptible to hackers gaining control.

Telegram's features made it a popular choice for activist groups and protesters in countries spanning from Brazil to Iran, and Germany to Ecuador. When Brazil blocked WhatsApp in December the app was downloaded 1 million downloads in a single day (Sawers, 2016). Many dissidents and activists turned to Telegram after Facebook acquired WhatsApp for fear of data mining and surveillance from the parent company (Hamburger, 2014). The app's features allow users to form groups and communities on the platform spanning countries and crossing borders. Being able to share sensitive files and messages on the app is a crucial feature that has made it so popular with activists the world over.

Pavel Durov, one of the founders of the app states that, "The No. 1 reason for me to support and help launch Telegram was to build a means of communication that cannot be accessed by the Russian security agencies, so I can talk about it for hours" (Sharkov, 2017). Ironically enough officials in the Russian government, including Putin's closest advisers use the app. The app has been criticised for being used by terrorist organisations operating on Russian territory and there are on-going attempts to ban the app. One of the biggest criticisms levelled against the app is its use by ISIS militants to recruit and organise their actions. Law enforcement officials and security agencies against the use of encryption have cited this as a reason to put restrictions on encrypted messaging apps. However, policy makers and human rights advocates have pointed out several times that mass restrictions harm the majority more than it prevents the minority offenders. Actions such as mass restriction of encrypted technologies and bans on secure messaging apps would violate the human rights of the larger part of the world's population than it would deter organised criminals and terrorists from carrying out their actions. On the technical side of things, users are still left vulnerable to surveillance since Telegram collects and stores messages, photos, and documents that are sent on chat (not secret chat, which has end-to-end encryption). The app also accesses users' contact list in order to alert users when a contact joins the app.

FireChat

FireChat was developed by San Francisco based startup Open Garden. The app operates on the basis of wireless mesh networking. Users can send messages to each other in the absence of Internet connectivity and cellular data, making use of peer to peer connectivity. Each device, with its wifi and Bluetooth connections switched on, becomes a node, transmitting signals to the devices around it, thereby allowing users to send messages. The higher the number of devices connected, the larger the network, and the better it functions. Devices need to be within a 70m radius of each other, therefore it works well in dense environments, like music festivals and demonstrations. This would explain why the app is popular in countries like Brazil, India, and Taiwan, where device penetration is high but Internet connectivity intermittent. The app is popularly used at events like Burning Man, an arts and music festival held in the Arizona desert in USA, music festivals the world over, during natural disasters and emergency situations, and most famously during the Umbrella Revolution in Hong Kong in 2014.

FireChat is different from the other apps in that it works via bluetooth and does not require an Internet connection. It is ideal for use in times of natural disasters or in crowded places where signal may be jammed. However a group of people need to be using to it for it to be effective.

Users download the app and create an account, using either their real names or pseudonyms. Public chat rooms can be created where users in the vicinity can enter the conversation. Private encrypted messages can also be sent, a feature that was introduced recently. When a user sends a private message to more than one contact, a private group is automatically created. Users can send messages to their own contacts, those nearby, or to everyone in a public chat room.

FireChat was developed as "proof of concept" but has proved itself quite indispensable in a number of situations including during the 2014 Umbrella Protest in Hong Kong.

FireChat has been instrumental to a number of protest movements, the most high profile being the pro-democracy Hong Kong protests in 2014. Although the Hong Kong protests were galvanised on WhatsApp groups and Facebook, protesters quickly switched to FireChat fearing an Internet shutdown would throw the movement into disarray. Although this did not happen, the app still proved itself pertinent since protesters could communicate even with the dense crowds and overloaded signals. Call for essential supplies and things that happened in real time quickly spread through the mesh network. Participants at the demonstration stated that rumours could be separated from the actual truth via FireChat (Toor, 2014). Since most users used pseudonyms it was easy to keep identities concealed from authorities although technically even authorities could have been present in the chat rooms. FireChat had not yet introduced encrypted messaging at this point. The app was downloaded 2,00,000 times in one day around a week after the protests started.

FireChat has proved itself indispensable during student protests in other parts of the world as well. Students and other young protesters used the app, although in much smaller numbers, during the Sunflower Student Movement in Taiwan. The protest was led by student groups and civic society organisations to protest the easing of trade restrictions with China that were passed by the ruling party, Kuomintang, in the absence of review of the clauses. Attendees of the rally were advised to download FireChat in case Internet connectivity was lost in a blog post on TechOrange, a leading Tech blog in Taiwan. Although Internet connectivity was not lost or disconnected during these two protests, it offered participants an alternative for communication and organisation in case of state repression. An interesting aftermath of FireChat's role during the Sunflower movement was the conversation it inspired between Taiwanese residents and those from Mainland China about the nature of freedom (Horwitz, 2014). Open Garden's algorithms group China, Hong Kong, and

Taiwan under the same geographical group. As a result, users were able to chat with people from all three regions in the public chat room that showed 'Everyone'. This rare conversation and assembly was facilitated by tools that enable open conversation, emphasising once again the importance of the free and secure communications for the right to assemble and associate.

FireChat was widely used in India during the floods in Kashmir in April 2015 and in Chennai in October 2015. After heavy rain caused major flooding and cut off mobile signals for a significant number of days, private citizens, aid workers, and NGOs used the app to co-ordinate rescue missions and distribute essential items using the app. Open Garden has released a feature that allows NGOs, organisations, and government departments to broadcast alerts to very many recipient using its new Alert feature. The company showcased the app and the feature at the United Nations World Humanitarian Summit in Istanbul in 2016 (Biswas, 2016). The many situations in which FireChat has been instrumental has alerted developers, non-profits, and disaster management officials of the need to create apps that can alleviate disaster situations.

The creators of the app built it as a mere "proof of concept", and did not expect it to become as popular as it has become (Horwitz, 2017). It is the nature of technology that it is taken by users and put to uses that it may not have been intended for. Some optimistic technologists have opined that the future of the Internet should move towards a decentralised control of Internet servers and a distributed system like peer-to-peer and mesh networks. This would mean that more people will have access to the Internet and be free from control by State or corporate actors. However, this does not negate the need for the protection of privacy and confidential communication. The app has introduced encryption and its future development seems to be headed in a direction quite different from its origins. Technological developments and innovations like this are the need of the hour in the face of ever increasing surveillance, control over Internet infrastructures, and greedy corporate interests.

SECURE COMMUNICATIONS IN INDIA

India by sheer dint of its population has one of the highest numbers of social media users. WhatsApp and Facebook Messenger, both owned by Facebook are the most popular messaging apps, although the two are not the most secure, leaving users vulnerable to data mining by the platform.

Popular social movements in India of the past few years like the Jan Lokpal movement, student protests in Jawaharlal Nehru University and Jadavpur University, or the few protests for women's safety have mobilised online, taken place in physical places, and spread through social media. Social media platforms like Facebook, Twitter, and WhatsApp have proven invaluable to disseminate information and mobilise citizens to act during times of natural disasters, social movements, and political protest.

In India, these three platforms are the most popular although the user demographic of these platforms differs. Facebook and WhatsApp are the most widely used, with Facebook reporting a potential audience of 241 million active users in India in July 2017 (PTI, 2017) and WhatsApp reporting 200 million monthly active users in February 2017 (Singh, 2017). Although social media penetration in India stands at just 19 per cent, the number of users has surpassed that in the USA and this number is only set to rise as more people get connected. For a majority of new users of social media, WhatsApp is usually the first platform they join and use, followed by Facebook. Twitter has a largely English language user base, although in recent years it has become extremely popular for citizens to follow politicians and government departments and seek information and news. Because of the breaking news nature of the platform, it functions as the first point of information for new developments in news, politics, natural disasters, etc. Only 13.7 per cent of social media users in India user Twitter with 23.2 million monthly active users (Jain, 2016).

Most lay users of social media and messaging platforms use the platforms to communicate with friends and loved ones, share photographs, and make voice over

Internet protocol (VoIP) calls. On these corporate platforms, the privacy settings offered by the companies are the only ones they can depend on to keep their communications secure. Their "encrypted" messages on these platforms may be protected against external parties but knowing the extent of their data mining practices and the economic profit that lies in selling this data, communications do not remain entirely secret or secure. Edward Snowden's revelations lifted the lid off private corporations' compliance and entrenched complicity in the NSA's activities. Therefore, WhatsApp's encrypted messaging or Facebook's Secret Messenger app cannot be considered secure communication. Apple and the FBI were recently involved in a headlock over Apple's refusal to hand over encryption keys to the FBI to aid in the San Bernardino bombing case. Apple stood its ground, refusing to allow any form of backdoor entry to its data and won the applause of advocates for privacy and encryption. Had Apple agreed to do allow the FBI a backdoor, it would have created a dangerous precedent. However, Apple's intentions need to be measured against its economic stake in the game.

The use of secure messaging applications like Signal, encrypted email tools like PGP keys, Tor browsers, and Virtual Private Networks (VPN) are relegated to the small minority whose work depends on secure communications like human rights defenders, activists, security specialists, and officials working on sensitive data. Even among this small minority, knowledge of digital tools to ensure secure communications is limited to the savvy few who are digitally adept.

ENCRYPTED APPS AND THEIR POTENTIAL USE IN INDIA

It comes as little surprise that encrypted messaging apps are not very popular nor have they seen widespread adoption. There are a number of reasons for this. While mobile penetration in India is comparably high in urban and semi-urban areas, the majority of people in rural

A large number of mobile users in India use basic Chinese or Indian devices that do not have adequate security features. Awareness about threats to security and privacy are low among users.

India use feature phones that have no provisions for encryption. Cheap devices, primarily Indian or Chinese made, have proliferated into the Indian market and these devices usually have limited security capabilities. Secure messaging applications like Signal, Wire, and FireChat cannot run on these phones and users must rely on service providers and the makers of devices to protect their communications. Another issue is that people use old devices that do not support the newer operating systems and the frequent change-over of new versions and advances makes devices obsolete very quickly. The proliferation of affordable Chinese and Indian made devices is a reason for this. These phones do not have good security features and although a majority run on Android operating system and should allow apps like Signal and FireChat to function, there are glaring cracks in the construction of phones that leave much to be desired in terms of security. Many users use old model devices that do not support newer versions of operating systems or new updates of applications. The population of people that use such phones are usually made up of taxi drivers to operate Uber, Ola, or other ride-sharing services, and those dwelling in semi-urban areas using basic banking and messaging apps. They usually have little knowledge of the perils of unprotected data or the risks of data leaks.

Social movements or student protests in India have not used digital technologies in the widespread way that say the Arab Spring or the Umbrella Revolution did. The agitation in Jawaharlal Nehru University in 2016 following protests against the hanging of Afzal Guru which led to arrest of student leader Kanhaiya Kumar or the protests at Hyderabad University against casteism were mobilised on the ground. Protesters occupied physical spaces and communication lines were not threatened during these protests. These protests were featured heavily in the Indian Twitter-verse and many a Facebook status was dedicated to it. However, the question of anonymity or secure communications did not become a majority concern throughout the duration of these protests. An app like FireChat would definitely have been useful had the threat of an Internet shutdown loomed large. Secure communications should be encouraged in similar cases to protect protesters from such implications.

There hasn't been any recorded case where secure communication app similar to the ones mentioned above were used in social movements and protests in India. There have been a number of movements and protests that were organised and ignited on public social media platforms like Twitter and Facebook.

STATE OF SECURE COMMUNICATIONS IN INDIA

Grassroots activists in Orissa

In a recently concluded workshop on secure communication conducted to benefit grassroots activists in Orissa, it was found that activists were aware of digital tools but were unsure of how to use them. The training covered secure messaging apps like Signal, Line, and Wire and how to use them to inform their activities. The two major drawbacks that people faced were poor connectivity and using outdated handsets.

The activists for whom the workshop was conducted worked against major corporations to protect their land and livelihood against illegal land grabbing and compensation. They required secure communications mainly to contact their funders and each other, while evading surveillance from police and corporations active in the area. Their main method of operation was to use coded messaging and sending locked files. Having access to a platform like Signal or Wire would ease their communications greatly. Not being digital natives, the activists had to be trained to download the app on their devices, install it, register, add contacts, verify the authenticity, and finally to use to chat securely. The biggest worry for them was the poor network connectivity in the areas they lived or worked and the app not working on some devices as they were too old to operate the application. A secure communication app like Signal for all its features and advantages requires data connectivity to function, and is rendered useless in the absence of such. An alternative to this is to use a mesh network application like FireChat which does not require Internet connectivity but does require that all users be physically close together to use it.

In India, the lack of awareness of alternatives and the lack of infrastructure put citizens in a vulnerable situation. To participate in a grassroots movement, it is pertinent that activists can communicate securely. However, bringing awareness to the issues they are fighting for requires concerted efforts on social media and public platforms to spread the word.

Jadavpur University student protests

The past few years have seen a number of student protests erupt across the country. In 2014, the hashtag #Hokkolorob (Let there be clamour) started inundating social media users' feeds in the city of Kolkata. #Hokkolorob was initiated to mobilise support as students – current and past - professors, and research scholars called for the resignation of the Vice Chancellor and Registrar following their ill-handling of a sexual assault complaint by a female student of the university. On the night of August 28th 2014, during the annual cultural festival Sanskriti, a second year undergraduate student and her friend were allegedly molested and assaulted by a group of students. She took the matter to the authorities who treated her complaint with gross indifference. The student filed an FIR after having facing apathy from the authorities and biased actions from the Internal Complaint Cell of the university. The student body organised an indefinite sit in on September 10th during the general body meeting in front of the main administration building. The situation reached boiling point when police were called to disperse the gathered students, against whom brutal force was used, and many accusations of sexual harassment were levelled against state authorities. This mobilised students to protest and the hashtag #Hokkolorob (to create cacophony) was created on Twitter to mobilise more participants. Students from other universities marched and were joined by professors old and new, alumni, and residents of the city to protest against the high handedness of

Jadavpur University authorities. Several students took to social media platforms to show their solidarity and support, and many calls to action were made. Because most participants were in the demographic that use social media the most, these calls were successful and the movement gained momentum and was supported by students across the country.

The use of secure communication apps by organisers of social movements and protests is minimal in India. Their use is limited to activists and human rights defenders in relatively urban areas. The existence of these apps and ways to use them must be publicised.

While social movements seem to erupt almost spontaneously as a result of a combination of factors, mobilising people and planning physical demonstrations take immense planning and coordination. Social media and public platforms are ideal for publicity and mobilising the masses, but planning and coordination between organisers require secure lines of communication and the assurance that their moves will not be used against them at a later date. Private communications are essential for activists and human rights defenders for whom threats against their causes and their personal safety is of high priority. Although the threat of an Internet shutdown was not immediate during the #Hokkolorob protests, mobile connections tend to get overloaded in crowded spaces leading to poor connectivity and difficulties in communicating. FireChat which functions via a mesh network would have been an ideal app if mobile Internet connections were spotty. With its encrypted messages feature, this would have ensured the privacy of protesters taking part in the movement from the threat of police action.

The protests at Jawaharlal Nehru University following the altercation between student groups and authorities after the protests against the capital punishment meted out to Afzal Guru, convicted of the 2001 Indian Parliament Attack, and Maqbool Bhat, a Kashmiri separatist devolved into accusations of anti-national sloganeering is another example where student protesters would have found secure messaging applications useful. Although this was not a typical social media movement, and the students who were singled out and further targeted were picked for their physical involvement in demonstrations, secure communication tools may have helped them keep in contact with family and loved ones when they went into hiding.

Planning protests, demonstrations, and coordination of actions for social movement take place at two levels – one, coordination and planning between small group of organisers or leaders of the movement, and two, mobilisation and publicity on social media. Because the public facing mobilisation efforts are highly visible and information is disseminated at an unprecedented speed thanks to social media, it is wrongly assumed that social movements in the social media age are largely leaderless. Social media platforms allow the engineering of spontaneity and inclusiveness, leaving the planning and coordination efforts largely unseen. It is these efforts that require secure communication avenues so that surveillance over organisers is prevented and all citizens may enjoy their freedoms and their ability to exercise their rights.

CONCLUSION

There is a dire need to promote secure communications in India and an even greater need to make these tools available to those in need. Only a small fraction of users are aware of secure communications and the need to incorporate such tools to their repertoire. While activists working at the grassroots know of secure communication tools, it is unlikely that they have the tools or means to update their knowledge or skill sets as updates and improvements are released periodically. Awareness among lay users of digital technologies is quite abysmal. In India, since a majority of users using mobile devices are first time users of any digital technology at all, issues of privacy and security take a back seat to learning how to operate the device. This difficulty is heightened by the fact that privacy is quite an alien concept in India and it does not occur to users to place high importance on security issues. Users are largely unaware of practices like data mining, vulnerabilities to hacks or the myriad ways in which corporate bodies could misuse personal information collected via apps and online activities.

Introducing secure communication tools and encouraging people to use them will require concerted efforts from civil society to educate and conduct awareness drives. It is important that a culture of safe use of digital technologies with emphasis on security and privacy is cultivated in users. The tools that currently exist, like the ones elucidated in the paper, may be the better options available to users now, but even these need to be monitored to ensure that diluted versions of them are not peddled to users. This is a risk in the technological ecosystem where smaller innovative players may be acquired by larger corporate interests and their qualities diluted. This is what happened when Skype, known to users for being secure, was acquired by Microsoft and many of its features were watered down.

Protecting the freedom of association and assembly online is incumbent on promoting the use of encryption technologies. However in India, this needs to be preceded by organised drives to create awareness of the many risks of using digital technologies and the safeguards users can take to protect themselves from these actions.

REFERENCES

Biswas , S. (2016, May 23). FireChat Alerts lets organisations broadcast messages even when networks fail. Retrieved July, 2017, from http://www.hindustantimes.com/tech/firechat-alerts-lets-organisations-broadcast-messages-even-when-networks-fail/story-NN8RCGUrJ8Bbl20hDhkm6N.html

February 23). Mobile messaging app Telegram passes 100 million monthly active users, a 60% increase in 9 months. Retrieved 2017, from https://venturebeat.com/2016/02/23/telegram-now-has-100-million-monthly-active-users-a-60-increase-in-9-months/

Field Fisher Waterhouse. (2013) The legal obligations for encryption of personal data in Europe and Asia (Rep.). (n.d.). Retrieved September 15, 2017, from Field Fisher Waterhouse website: http://www.infosecurityeurope.com/__novadocuments/21997

Hamburger, E. (2014, February 25). Why Telegram has become the hottest messaging app in the world. Retrieved July, 2017, from https://www.theverge.com/2014/2/25/5445864/telegram-messenger-hottest-app-in-the-world

Horwitz, J. (2014, March 31). Unblockable? Unstoppable? FireChat messaging app unites China and Taiwan in free speech… and it's not pretty. Retrieved July, 2017, from https://www.techinasia.com/unblockable-unstoppable-firechat-messaging-app-unites-china-and-taiwan-in-free-speech-and-its-not-pretty

Jain, S. (2016, December 16). 101 Latest Social Media Facts and Stats from India - 2016 | Digital Marketing Facts. Retrieved July, 2017, from http://www.soravjain.com/social-media-facts-and-stats-india-2016

Kalathil, S., & Boas, T. C. (2003). Open networks, closed regimes: the impact of the Internet on authoritarian rule.

Medeiros, F. A., & Bygrave, L. A. (2015). Brazils Marco Civil da Internet: Does it live up to the hype? Computer Law & Security Review, 31(1), 120-130. doi:10.1016/j.clsr.2014.12.001

Phys.org. (2017, June 22). Germany expands surveillance of *encrypted message services. Retrieved July 2017, from https://phys.org/news/2017-06-germany-surveillance-encrypted-message.html*

PTI. (2017, July 14). India now has highest number of Facebook users, beats US: Report. Retrieved July, 2017, from http://www.livemint.com/Consumer/CyEKdaltF64YycZsU72oEK/Indians-largest-audience-country-for-Facebook-Report.html

Sawers, P. (2016, Privacy International. (2017, July 26). State of Privacy India. Retrieved July 2017, from https://www.privacyinternational.org/node/975

Sharkov, D. (2017, June 27). Will Russia ban Telegram-the app ISIS uses, Russians love and governments hate? Retrieved July, 2017, from http://www.newsweek.com/what-telegram-app-isis-uses-russians-love-and-governments-hate-629326

Schulz, W., & Hoboken, J. V. (2016). Human rights and encryption (Publication). Paris: UNESCO.

Singh, M. (2017, February 24). WhatsApp hits 200 million active users in India. Retrieved July 2017, from http://mashable.com/2017/02/24/whatsapp-india-200-million-active-users/#QapHLMS7ssqp

Smiley, L. (2017, January 12). Signal Boost: Demand for secret messaging apps is rising as Trump takes office. Retrieved July, 2017, from https://www.theverge.com/2017/1/12/14244634/signal-app-secure-messaging-trump-surveillance-encryption

Tracol, X. (2015). Back to basics: The European Court of Justice further defined the concept of personal data and the scope of the right of data subjects to access it. Computer Law & Security Review, 31(1), 112-119. doi:10.1016/j.clsr.2014.11.007

Toor, A. (2014, October 16). Why a messaging app meant for festivals became massively popular during Hong Kong protests. Retrieved July, 2017, from https://www.theverge.com/2014/10/16/6981127/firechat-messaging-app-accidental-protest-app-hong-kong

PROTECTING FOAA ONLINE

WITH ENCRYPTION TECHNOLOGIES

Social media platforms are fast becoming the preferred mode of organising social protests and movements for their convenience and ability to reach large audiences. Protecting user data with encryption technologies has become essential to protecting human rights online. This report explores the importance of encryption technologies to protect FoAA online.

European Union

APC IMPACT
India . Malaysia . Pakistan
Advocacy for Change Through Technology

DEF
DIGITAL EMPOWERMENT foundation