IN THE HIGH COURT OF JUDICATURE AT MADRAS

(Special Original Jurisdiction)

W.P. Nos. 20774 & 20214 of 2019

Antony Clement Rubin ...Petitioner

[in W.P No. 20774 of 2019]

And

Janani Krishnamurthy ...Petitioner

[in W.P No. 20214 of 2019]

--VS--

Union of India & Others ...Respondents

INDEX TO TYPED SET OF DOCUMENTS VOLUME- II

S. NO.	DATE	PARTICULARS	PAGE NO.
1.	20.08.2019	Copy of Dr. Prabhakaran's Technical Opinion on Dr. Kamakoti's proposal	1
2.	22.05.2015	UN Special Rapporteur's Report on Encryption, Anonymity and the Human Rights Framework (UN Doc A/HRC/29/32)	8

Certified that the above are true copies of originals.

Dated at Chennai on this, the 21st day of August, 2019

COUNSEL FOR INTERVENOR /R15

INTERNET FREEDOM FOUNDATION

Devdutta Mukhopadhyay <devdutta@internetfreedom.in>

Technical opinion regarding Dr. Kamakoti's proposal to introduce traceability on encrypted platforms

Manoj M Prabhakaran <mp@cse.iitb.ac.in> Tue, Aug 20, 2019 at 10:53 AM
To: Apar Gupta <apar@internetfreedom.in>
Cc: Devdutta Mukhopadhyay <devdutta@internetfreedom.in>

Dear Apar, Devdutta,

I am currently the Vijay and Sita Vashee chair Professor in the Department of Computer Science and Engineering at the Indian Institute of Technology (IIT) Bombay. My research expertise spans cryptography and information security, and various topics in theoretical computer science and information theory. Prior to joining IIT Bombay I was an Assistant/Associate Professor of Computer Science at the University of Illinois, Urbana-Champaign, from 2005 to 2016, where I advised Ph.D. students who are now themselves well established researchers in cryptography and information security. I received a Ph.D. in Computer Science from Princeton University in 2005, in the area of cryptography. I graduated from IIT Bombay in 2000, with a B.Tech in Computer Science and Engineering and the Institute Gold Medal. I have received an IBM Ph.D. Fellowship, an NSF CAREER award, a Beckman Faculty Fellowship, and a Ramanujan Fellowship. I am currently an Associate Editor of the Journal of Cryptology and a member of the steering committee for the Theory of Cryptography Conference.

Internet Freedom Foundation had reached out to me via email to provide an expert opinion on the technical feasibility of the proposal made by Dr. Kamakoti in Antony Clement Rubin v. Union of India (WP No. 20774 of 2018). I have gone through Dr. Kamakoti's proposal in detail and carefully considered its various technical aspects. With this email I am attaching my response which highlights certain concerns about the proposal.

I consent to Internet Freedom Foundation filing my technical response to Dr. Kamakoti's proposal as a part of their submission before the Hon'ble Madras High Court. I hope that these inputs will provide greater clarity and insight to all stakeholders.

Regards,
Manoj
--
Manoj M Prabhakaran : Computer Science and Engineering
Professor : Indian Institute of Technology Bombay

whatsapp-comments.pdf
72K

2

On a Proposal for Originator Tracing in WhatsApp

Manoj Prabhakaran

IIT Bombay

Abstract

This is a comment on a proposal by V. Kamakoti [1] on how the popular messaging application WhatsApp could be modified by its vendors (Facebook) to help trace the originator of a message that has gone viral. We comment on some implications and the effectiveness of the proposal. In particular, we point out that (1) in the current proposal, the originator information is open to spoofing, but this can be mitigated to a reasonable extent by employing digital signatures, (2) the proposal will have a deleterious effect on the privacy of (common) users, which can again be partly addressed by slightly modifying the proposal, and (3) the effectiveness of the proposed mechanism (with or without the suggested modifications) is likely to be very limited.

Background

WhatsApp allows users to receive messages from other users who are connected to them directly (both know each other's phone number) or via "groups" that they are part of [2]. Viral messages are known to spread through this Whatsapp network. To deter propagation of maliciously crafted messages, it has been proposed that information identifying the phone number from which the original message is posted should be included as part of the message's metadata. Kamakoti's note [1] outlines two versions of this suggestion -- one in which this metadata is available in the clear to everyone receiving the message, and one in which the metadata is kept encrypted so that it can be decrypted only using a key held in escrow (by Facebook itself, in the proposal).

3

Room for Impersonation and Possible Mitigation

An important consideration, which is not mentioned in the proposal, is whether the identifying information recovered from a viral message can be trusted to be authentic. Note that the original message may not be created using the official WhatsApp client, but a malicious client (possibly obtained by reverse engineering and modifying the official client). This allows the originator to include arbitrary data instead of the identifying information captured using the device.

This concern can be addressed using *digital signatures*, so that an honest user cannot be implicated by a corrupt user (see below). However, the only piece of information that is authenticated is the phone number used by the client as their registration information in the WhatsApp system.

Mitigation

When a client app registers with the WhatsApp server, it sends a public "Identity Key" which corresponds to a secret signing key generated by the client [2]. An honest client is cryptographically guaranteed that only it can create digital signatures for a message that will match with its Identity Key. Also, the WhatsApp server ensures that the Identity Key is associated with a phone number that can be accessed by the user carrying out the registration (via a one-time password). (WhatsApp client also may collect other information from the user's device and send it to the WhatsApp server. However, this information cannot be trusted if the client is malicious.)

To protect against implicating an honest user as the originator of a message they did not create, we can require that the originator information in the message includes a digital signature of the message. An honest client (whose signing keys are not stolen) can rest assured that no one else can forge the signature using their registered Identity Key (due to cryptographic security of the signature scheme) or register a different key against their phone number (due to the one-time password).[1]

[1] A technicality here is that the Identity Key gets changed when a user registers a new client (say, by reinstalling the app). We will need WhatsApp servers to retain historical Identity Keys for a few months after they are changed.

This guarantee ***does not hold*** if the honest user's signing keys are stolen (e.g., via a malware in their phone) or if their one-time password is compromised. In particular, the guarantee does not hold if the attacker has access to the SMS network (telecom operators, government agencies). As such, the originator information ***should not have any evidentiary value,*** but may be of value to investigative agencies.

Implications to Privacy

It may be argued that someone creating a viral message should have no expectation of anonymity, and should be responsible for its contents. However, if someone creates a *personal* message to another party, or to a small closed group, they can reasonably expect privacy, due to guarantees enshrined in the constitution. Mandating that their identity is attached to every message that they create will have a chilling effect on the right to free speech.

Incidentally, our suggestion above for mitigating the possibility of false implication, exacerbates the situation. In an end-to-end encrypted conversation, which forms a key feature of WhatsApp, the participants may naturally expect that their conversation is "off-the-record" so that even if one party later publishes their private conversation, the other party can deny its veracity. (One of the original motivations behind cryptographic protocols that later evolved into the one used in WhatsApp is the need for "off-the-record" messaging.) Attaching signatures would make such denial harder.

Mitigation

This issue can be somewhat mitigated by allowing users to designate any message he or she sends as "not for sharing." The WhatsApp client will then not include the originator information, and also will not allow the recipients to forward/share those messages.[2] The users may be accorded somewhat finer control too. Rather than designating their messages as not for sharing, they can designate it as "for limited sharing", which may limit the length of a chain in which the message can be forwarded (to 2, say).

[2] It has been brought to our attention that a similar idea has been proposed by Kamakoti [3].

5

Note that with some effort the recipients of such a message can create a new message with the original contents and send it to anyone. The message itself may include a request to the reader to download it and resend it as not for sharing. Nevertheless, we believe that this presents as much barrier to making a message viral as the original mechanism does (which, as we argue below, is not much).

Another measure towards mitigating privacy concerns is that the originator information will be maintained encrypted so that it can be decrypted only if a watchdog agency cooperates to reveal it. A version of this is suggested in Kamakoti's original proposal [1], where the watchdog's role is played by WhatsApp (Facebook) itself. A more robust version (which can also be easily implemented using standard cryptographic tools) would allow a panel of watchdog agencies all (or some) of whom must cooperate to recover this information. If responsible international agencies who are all unlikely to be influenced by a single country's government join this panel, it would not only reassure the users, but also protect Facebook from undue pressure that a government can place it under.

Effectiveness

The effectiveness of the proposed method is limited. There are several workarounds that suggest themselves.

1. Firstly, by using a reverse-engineered WhatsApp client, the only originator information that would be reliable would be the phone number. This information has little identification value, since it is easy to anonymously acquire (international) phone numbers, either directly from international telecom operators, or via services like Google Voice, Skype and Viber.
2. Even without access to a reverse-engineered WhatsApp client, one can hire (say) thousands of workers to serve as the originators; even if some of the workers are traced, their employer can remain untraceable. (The workers may take the risk of being traced due to lack of awareness, because the compensation is attractive enough to overcome their concerns, or simply because they are operating from a jurisdiction where their actions are not illegal.)
3. While the above attacks required a well funded adversary, one can expect that if originator tracing is a significant concern, then services for creating untraceable

messages would become *commercially* available making it easy for anyone to avoid tracing. A user could simply send the desired message via email[3] to an international service provider, who would send it back to the user via WhatsApp, with themselves as the originator. The user then proceeds to *forward* it to groups/individuals (without becoming the originator).[4]

Finally, it is not clear if traceability serves as much of a deterrence, given the prevalence of fake news spread openly through platforms like Twitter, Facebook, websites and even mass media.

On the other hand, for viral messages originating from users with limited resources, the proposed mechanisms may work well, at least until commercial services for circumventing them become widely available.

Conclusion

Including a mechanism for tracing the originator (that can be optionally turned off, for messages not intended for sharing) is a relatively mild modification, and in the short term, could be effective in deterring some individual actors from creating viral messages that the law enforcement authorities find objectionable. But it has very limited effectiveness in the long term, or against determined attackers.

We note that more effective alternatives may exist. Viral messages (not the users) could be "outed" and made available publicly so that fact checkers could add comments to them, and the WhatsApp client can display these comments alongside the messages. To implement this, an optional feature could let users identify messages they have received after several forwards (as estimated using a counter maintained within the message), and anonymously communicate[5] those messages to a server for making them available publicly. It may also be possible to design offline or online "spam filters," which can detect and mark messages as potentially unreliable, to discourage users from sharing them. For a

[3] The user could use WhatsApp itself to communicate with the service provider. However, since the service provider's WhatsApp accounts are at risk of being banned by WhatsApp and may keep changing, an alternate means of communication would be more robust.
[4] Even if entire paths, instead of just the origin, is to be traced, the service provider can shield the actual originator, by directly spreading the message to groups suggested by the user.
[5] Anonymous communication can be achieved via an existing infrastructure like "Tor" or via a dedicated "mix network" operated by independent service providers.

7

company like Facebook it would be easy to quickly develop such a mechanism (and incrementally improve its effectiveness), with minimal disruption to the user experience.

Finally, there is increasing recognition that a lasting defence against the spread of fake news should be based on education and information literacy [4][5]. Such efforts should complement technological and legal attempts to regulate the online world.

References

1. V. Kamakoti, Report on Originator Traceability in WhatsApp Messages, July 2019. https://archive.org/details/reportofprof.kamakotiinwpnos.20214and20774of2018
2. "WhatsApp Encryption Overview: Technical white paper," December 2017. https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf
3. Aditi Agrawal, Nikhil Pahwa. "IIT Madras's Kamakoti tells MediaNama how WhatsApp traceability is possible without undermining end-to-end encryption". August 2019. https://www.medianama.com/2019/08/223-kamakoti-medianama-whatsapp-traceability-interview/
4. Kalev Leetaru, "A Reminder That 'Fake News' Is An Information Literacy Problem - Not A Technology Problem," Forbes, July 2019. https://www.forbes.com/sites/kalevleetaru/2019/07/07/a-reminder-that-fake-news-is-an-information-literacy-problem-not-a-technology-problem
5. P. Anima, "Kannur schoolchildren are leading the fight against online fake news." The Hindu Businessline, March 2019. https://www.thehindubusinessline.com/blink/know/debunking-class/article26606593.ece

Advance Edited Version

Distr.: General
22 May 2015

Original: English

Human Rights Council
Twenty-ninth session
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*

Summary

In the present report, submitted in accordance with Human Rights Council resolution 25/2, the Special Rapporteur addresses the use of encryption and anonymity in digital communications. Drawing from research on international and national norms and jurisprudence, and the input of States and civil society, the report concludes that encryption and anonymity enable individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection.

* Late submission.

Contents

I. Introduction

1. Contemporary digital technologies offer Governments, corporations, criminals and pranksters unprecedented capacity to interfere with the rights to freedom of opinion and expression. Online censorship, mass and targeted surveillance and data collection, digital attacks on civil society and repression resulting from online expression force individuals around the world to seek security to hold opinions without interference and seek, receive and impart information and ideas of all kinds. Many seek to protect their security through encryption, the scrambling of data so only intended recipients may access it, which may be applied to data in transit (e.g., e-mail, messaging, Internet telephony) and at rest (e.g., hard drives, cloud services). Others seek additional protection in anonymity, using sophisticated technologies to disguise their identity and digital footprint. Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression.

2. Yet, just as the telephone may be used both to report a crime to the police and to conspire to commit one, so too may the Internet be abused to interfere with the rights of others, national security or public order. Law enforcement and intelligence services often assert that anonymous or encrypted communications make it difficult to investigate financial crimes, illicit drugs, child pornography and terrorism. Individuals express legitimate concerns about how bullies and criminals use new technologies to facilitate harassment. Some States restrict or prohibit encryption and anonymity on these and other grounds, while others are proposing or implementing means for law enforcement to circumvent these protections and access individual communications.

3. In the light of these challenges, the present report examines two linked questions. First, do the rights to privacy and freedom of opinion and expression protect secure online communication, specifically by encryption or anonymity? And, second, assuming an affirmative answer, to what extent may Governments, in accordance with human rights law, impose restrictions on encryption and anonymity? The present report seeks to answer these questions, review examples of State practice and propose recommendations. It does not purport to address every technical or legal question raised by digital technologies, but it identifies important ones for future reporting.

4. In preparing the report, the Special Rapporteur circulated a questionnaire to States, seeking relevant information on their domestic laws, regulations, policies and practices. As of 1 April 2015, 16 States had responded to this request.[1] The Special Rapporteur also issued a call for submissions from non-governmental stakeholders and convened a meeting of experts in Geneva in March 2015. The responses from Governments and the over 30 submissions by civil society organizations and individuals, which are available from the mandate holder's web page, contributed significantly to the preparation of the report.

5. A full review of the Special Rapporteur's activities since the beginning of his term in August 2014 may be found on the mandate holder's web page. This report, the current mandate holder's first, aims at furthering the work on the challenges to freedom of expression in the digital age.

II. Secure and private communication in the digital age

A. Contemporary encryption and anonymity

6. Modern approaches to private and secure communication draw on ideas that have been with humankind for millenniums. The rise of electronic data storage, the Internet and mass data collection and retention made clear that sophisticated means would be needed to protect individual, corporate and government data. As e-mail, instant-messaging, Voice-over-Internet Protocols, videoconferencing and social media moved from niche services to predominant and easily monitored modes of communication, individuals developed a need for security online, so

[1] Responses were received from Austria, Bulgaria, Cuba, Germany, Greece, Guatemala, Ireland, Kazakhstan, Lebanon, Qatar, Republic of Moldova, Norway, Slovakia, Sweden, Turkey and the United States of America.

that they could seek, receive and impart information without the risk of repercussions, disclosure, surveillance or other improper use of their opinions and expression.

7. Encryption — a mathematical "process of converting messages, information, or data into a form unreadable by anyone except the intended recipient"[2] — protects the confidentiality and integrity of content against third-party access or manipulation. Strong encryption, once the sole province of militaries and intelligence services, is now publicly accessible and often freely available to secure e-mail, voice communication, images, hard drives and website browsers. With "public key encryption", the dominant form of end-to-end security for data in transit, the sender uses the recipient's public key to encrypt the message and its attachments, and the recipient uses her or his own private key to decrypt them. Encryption may also be used to create digital signatures to ensure that a document and its sender are authentic, to authenticate and verify the identity of a server and to protect the integrity of communications between clients against tampering or manipulation of traffic by third parties (e.g., "man-in-the-middle" attacks). Since the encryption of data in transit does not ensure against attacks on unencrypted data when it is sitting at rest at either endpoint (nor protect the security of one's private key), one may also encrypt data at rest stored on laptops, hard drives, servers, tablets, mobile phones and other devices. Online practices may also be moving away from the system described here and towards "forward secrecy" or "off-the-record" technology in which keys are held ephemerally, particularly for uses such as instant messaging.

8. Some call for efforts to weaken or compromise encryption standards such that only Governments may enjoy access to encrypted communications. However, compromised encryption cannot be kept secret from those with the skill to find and exploit the weak points, whether State or non-State, legitimate or criminal. It is a seemingly universal position among technologists that there is no special access that can be made available only to government authorities, even ones that, in principle, have the public interest in mind. In the contemporary technological environment, intentionally compromising encryption, even for arguably legitimate purposes, weakens everyone's security online.

9. Notably, encryption protects the content of communications but not identifying factors such as the Internet Protocol (IP) address, known as metadata. Third parties may gather significant information concerning an individual's identity through metadata analysis if the user does not employ anonymity tools. Anonymity is the condition of avoiding identification. A common human desire to protect one's identity from the crowd, anonymity may liberate a user to explore and impart ideas and opinions more than she would using her actual identity. Individuals online may adopt pseudonyms (or, for instance, fake e-mail or social media accounts) to hide their identities, image, voice, location and so forth, but the privacy afforded through such pseudonyms is superficial and easily disturbed by Governments or others with the necessary expertise; in the absence of combinations of encryption and anonymizing tools, the digital traces that users leave behind render their identities easily discoverable. Users seeking to ensure full anonymity or mask their identity (such as hiding the original IP address) against State or criminal intrusion may use tools such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks.[3] One well-known anonymity tool, the Tor network, deploys more than 6,000 decentralized computer servers around the world to receive and relay data multiple times so as to hide identifying information about the end points, creating strong anonymity for its users.

10. A key feature of the digital age is that technology changes incessantly to sate user demands. Although the present report refers to contemporary technologies that facilitate encryption and anonymity, its analysis and conclusions apply generally to the concepts behind the current technologies and should be applicable as new technologies replace the old.

B. Uses of the technologies

11. The Internet has profound value for freedom of opinion and expression, as it magnifies the voice and multiplies the information within reach of everyone who has access to it. Within a brief period, it has become the central global public forum. As such, an open and secure Internet should be counted among the leading prerequisites for the enjoyment of the freedom of expression today. But it is constantly under threat, a space — not unlike the physical world — in which criminal enterprise, targeted repression and mass data collection also exist. It is thus

[2] See SANS Institute, "History of encryption" (2001).

[3] Proxy services send data through an intermediary, or "proxy server", that sends that data on behalf of the user, effectively masking the user's IP address with its own to the end recipient. Peer-to-peer networks partition and store data among interconnected servers and then encrypt that stored data so that no centralized server has access to identifying information. See, for example, Freenet.

critical that individuals find ways to secure themselves online, that Governments provide such safety in law and policy and that corporate actors design, develop and market secure-by-default products and services. None of these imperatives is new. Early in the digital age, Governments recognized the essential role played by encryption in securing the global economy, using or encouraging its use to secure Government-issued identity numbers, credit card and banking information, business proprietary documents and investigations into online crime itself.[4]

12. Encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief. For instance, they enable private communications and can shield an opinion from outside scrutiny, particularly important in hostile political, social, religious and legal environments. Where States impose unlawful censorship through filtering and other technologies, the use of encryption and anonymity may empower individuals to circumvent barriers and access information and ideas without the intrusion of authorities. Journalists, researchers, lawyers and civil society rely on encryption and anonymity to shield themselves (and their sources, clients and partners) from surveillance and harassment. The ability to search the web, develop ideas and communicate securely may be the only way in which many can explore basic aspects of identity, such as one's gender, religion, ethnicity, national origin or sexuality. Artists rely on encryption and anonymity to safeguard and protect their right to expression, especially in situations where it is not only the State creating limitations but also society that does not tolerate unconventional opinions or expression.

13. The "dark" side of encryption and anonymity is a reflection of the fact that wrongdoing offline takes place online as well. Law enforcement and counter-terrorism officials express concern that terrorists and ordinary criminals use encryption and anonymity to hide their activities, making it difficult for Governments to prevent and conduct investigations into terrorism, the illegal drug trade, organized crime and child pornography, among other government objectives. Harassment and cyberbullying may rely on anonymity as a cowardly mask for discrimination, particularly against members of vulnerable groups. At the same time, however, law enforcement often uses the same tools to ensure their own operational security in undercover operations, while members of vulnerable groups may use the tools to ensure their privacy in the face of harassment. Moreover, Governments have at their disposal a broad set of alternative tools, such as wiretapping, geo-location and tracking, data-mining, traditional physical surveillance and many others, which strengthen contemporary law enforcement and counter-terrorism.[5]

III. Encryption, anonymity and the rights to freedom of opinion and expression and privacy

14. The human rights legal framework for encryption and anonymity requires, first, evaluating the scope of the rights at issue and their application to encryption and anonymity; and, second, assessing whether, and if so to what extent, restrictions may lawfully be placed on the use of technologies that promote and protect the rights to privacy and freedom of opinion and expression.

15. The rights to privacy[6] and freedom of opinion and expression[7] have been codified in universal and regional human rights instruments, interpreted by treaty bodies and regional courts, and evaluated by special procedures of the Human Rights Council and during universal periodic review. The universal standards for privacy, opinion and expression are found in the International Covenant on Civil and Political Rights, to which 168 States are party. Even for those remaining States that are not bound by it, the Covenant presents at the very least a standard for achievement and often reflects a customary legal norm; those that have signed but not ratified the Covenant are bound to respect its object and purpose under article 18 of the Vienna Convention on the Law of Treaties. National legal systems also protect privacy, opinion and expression, sometimes with constitutional or basic law or interpretations thereof. Several

[4] See OECD, *Guidelines for Cryptography Policy* (1997)..

[5] See Center for Democracy and Technology, "'Going Dark' versus a 'Golden Age for Surveillance'" (2011).

[6] Article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights, article 16 of the Convention on the Rights of the Child, article 22 of the Convention on the Rights of Persons with Disabilities, article 14 of the Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, article 8 of the European Convention on Human Rights and article 11 of the American Convention on Human Rights protect the right to privacy.

[7] Article 19 of the Universal Declaration and the International Covenant on Civil and Political Rights, article 9 of the African Charter on Human and Peoples' Rights, article 13 of the American Convention on Human Rights and article 10 of the European Convention on Human Rights protect freedom of expression.

13

global civil society projects have also provided compelling demonstrations of the law that should apply in the context of the digital age, such as the International Principles on the Application of Human Rights to Communications Surveillance and the Global Principles on National Security and the Right to Information. Although specific standards may vary from right to right, or instrument to instrument, a common thread in the law is that, because the rights to privacy and to freedom of expression are so foundational to human dignity and democratic governance, limitations must be narrowly drawn, established by law and applied strictly and only in exceptional circumstances. In a digital age, protecting such rights demands exceptional vigilance.

A. Privacy as a gateway for freedom of opinion and expression

16. Encryption and anonymity provide individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks. The previous mandate holder noted that the rights to "privacy and freedom of expression are interlinked" and found that encryption and anonymity are protected because of the critical role they can play in securing those rights (A/HRC/23/40 and Corr.1). Echoing article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights specifically protects the individual against "arbitrary or unlawful interference with his or her privacy, family, home or correspondence" and "unlawful attacks on his or her honour and reputation", and provides that "everyone has the right to the protection of the law against such interference or attacks". The General Assembly, the United Nations High Commissioner for Human Rights and special procedure mandate holders have recognized that privacy is a gateway to the enjoyment of other rights, particularly the freedom of opinion and expression (see General Assembly resolution 68/167, A/HRC/13/37 and Human Rights Council resolution 20/8).

17. Encryption and anonymity are especially useful for the development and sharing of opinions, which often occur through online correspondence such as e-mail, text messaging, and other online interactions. Encryption provides security so that individuals are able "to verify that their communications are received only by their intended recipients, without interference or alteration, and that the communications they receive are equally free from intrusion" (see A/HRC/23/40 and Corr.1, para. 23). Given the power of metadata analysis to specify "an individual's behaviour, social relationships, private preferences and identity" (see A/HRC/27/37, para. 19), anonymity may play a critical role in securing correspondence. Besides correspondence, international and regional mechanisms have interpreted privacy to involve a range of other circumstances as well.[8]

18. Individuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection. In article 17 (2) of the International Covenant on Civil and Political Rights, States are obliged to protect privacy against unlawful and arbitrary interference and attacks. Under such an affirmative obligation, States should ensure the existence of domestic legislation that prohibits unlawful and arbitrary interference and attacks on privacy, whether committed by government or non-governmental actors. Such protection must include the right to a remedy for a violation.[9] In order for the right to a remedy to be meaningful, individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data.

B. Right to hold opinions without interference

19. The first article of the Universal Declaration of Human Rights recognizes that everyone is "endowed with reason and conscience", a principle developed further in human rights law to include, among other things, the protection of opinion, expression, belief, and thought. Article 19 (1) of the International Covenant on Civil and Political Rights, also echoing the Universal Declaration, provides that "everyone shall have the right to hold opinions without interference". Opinion and expression are closely related to one another, as restrictions on the right to receive information and ideas may interfere with the ability to hold opinions, and interference with the holding of opinions necessarily restricts the expression of them. However, human rights law has drawn a conceptual distinction between the two. During the negotiations

[8] Human Rights Committee, general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation. See also European Court of Human Rights, factsheets on data protection (www.echr.coe.int/Documents/FS_Data_ENG.pdf) and right to protection of one's image (www.echr.coe.int/Documents/FS_Own_image_ENG.pdf).

[9] See Human Rights Committee general comment No.16 and general comment No. 31on the nature of the general legal obligation imposed on States parties to the Covenant; and CCPR/C/106/D/1803/2008.

on the drafting of the Covenant, "the freedom to form an opinion and to develop this by way of reasoning was held to be absolute and, in contrast to freedom of expression, not allowed to be restricted by law or other power".[10] The ability to hold an opinion freely was seen to be a fundamental element of human dignity and democratic self-governance, a guarantee so critical that the Covenant would allow no interference, limitation or restriction. Consequently, the permissible limitations in article 19 (3) expressly apply only to the right to freedom of expression in article 19 (2). Interference with the right to hold opinions is, by contrast, per se in violation of article 19 (1).

20. Commentators and courts have devoted much less attention to the right to hold opinions than to expression. Greater attention is warranted, however, as the mechanics of holding opinions have evolved in the digital age and exposed individuals to significant vulnerabilities. Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. In other words, holding opinions in the digital age is not an abstract concept limited to what may be in one's mind. And yet, today, holding opinions in digital space is under attack. Offline, interference with the right to hold an opinion may involve physical harassment, detention or subtler efforts to punish individuals for their opinion (see CCPR/C/78/D/878/1999, annex, paras. 2.5, 7.2 and 7.3). Interference may also include such efforts as targeted surveillance, distributed denial of service attacks, and online and offline intimidation, criminalization and harassment. Targeted digital interference harasses individuals and civil society organizations for the opinions they hold in many formats. Encryption and anonymity enable individuals to avoid or mitigate such harassment.

21. The right to hold opinions without interference also includes the right to form opinions. Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity, such as search and browsing, likely deters individuals from accessing information, particularly where such surveillance leads to repressive outcomes. For all these reasons, restrictions on encryption and anonymity must be assessed to determine whether they would amount to an impermissible interference with the right to hold opinions.

C. Right to freedom of expression

22. The right to freedom of expression under article 19 (2) of the International Covenant on Civil and Political Rights expands upon the Universal Declaration's already broad guarantee, protecting the "freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". A significant accumulation of jurisprudence, special procedure reporting, and resolutions within the United Nations and regional human rights systems underscores that the freedom of expression "is essential for the enjoyment of other human rights and freedoms and constitutes a fundamental pillar for building a democratic society and strengthening democracy" (Human Rights Council resolution 25/2). The Human Rights Council, the General Assembly and individual States regularly assert that individuals enjoy the same rights online that they enjoy offline.[11] The present report will not repeat all the elements of this consensus. In the context of encryption and anonymity, three aspects of the text deserve particular emphasis (see paras. 23–26 below).

23. **Freedom to seek, receive, and impart information and ideas:** In environments of prevalent censorship, individuals may be forced to rely on encryption and anonymity in order to circumvent restrictions and exercise the right to seek, receive and impart information. Some States have curtailed access with a variety of tools. State censorship, for instance, poses sometimes insurmountable barriers to the right to access information. Some States impose content-based, often discriminatory restrictions or criminalize online expression, intimidating political opposition and dissenters and applying defamation and lese-majesty laws to silence journalists, defenders and activists. A VPN connection, or use of Tor or a proxy server, combined with encryption, may be the only way in which an individual is able to access or share information in such environments.

[10] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), p. 441.

[11] See, e.g., General Assembly resolution 68/167, Human Rights Council resolution 26/13 and Council of Europe recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a guide to human rights for Internet users.

24. It bears emphasizing that human rights law also protects the right to seek, receive and impart scientific information and ideas. The Universal Declaration and the International Covenant on Economic, Social and Cultural Rights protect rights to education and "to share in scientific advancement and its benefits". Encryption and anonymity technologies enable individuals to share in such information in situations where they are otherwise denied, and they are themselves examples of scientific advancement. Their use empowers individuals to gain access to the benefits of scientific progress that might be curtailed by Government. The Special Rapporteur in the field of cultural rights noted that "the rights to science and to culture should both be understood as including a right to have access to and use information and communication and other technologies in self-determined and empowering ways" (see A/HRC/20/26, para. 19).

25. **Regardless of frontiers:** The major instruments guaranteeing freedom of expression explicitly acknowledge the transboundary scope of the right. Individuals enjoy the right to receive information from, and transmit information and ideas of all kinds to, places beyond their borders.[12] However, some States filter or block data on the basis of keywords, denying access by deploying technologies that rely on access to text. Encryption enables an individual to avoid such filtering, allowing information to flow across borders. Moreover, individuals do not control — and are usually unaware of — how or if their communications cross borders. Encryption and anonymity may protect information of all individuals as it transits through servers located in third countries that filter content.

26. **Through any media:** Articles 19 of the Universal Declaration and the International Covenant on Civil and Political Rights were drafted with the foresight to accommodate future technological advances (A/HRC/17/27). The States parties to the Covenant chose to adopt the general phrase "through any other media" as opposed to an enumeration of then-existing media. Partly on this basis, international mechanisms have repeatedly acknowledged that the protections of freedom of expression apply to activities on the Internet. Regional courts have likewise recognized that protections apply online.[13] The European Court of Human Rights, in discussing the similar protection of expression in the European Convention for the Protection of Human Rights and Fundamental Freedoms, has indicated that the forms and means through which information is transmitted and received are themselves protected, since any restriction imposed on the means necessarily interferes with the right to receive and impart information.[14] In this sense, encryption and anonymity technologies are specific media through which individuals exercise their freedom of expression.

D. Roles of corporations

27. Corporations in a variety of sectors play roles in advancing or interfering with privacy, opinion and expression, including encryption and anonymity. Much online communication (and virtually all of it in some countries) is carried on networks owned and operated by private corporations, while other corporations own and manage websites with substantial user-generated content. Others are active players in the surveillance and spyware markets, providing hardware and software to Governments to compromise the security of individuals online. Others develop and provide services for secure and private online storage. Telecommunications entities, Internet service providers, search engines, cloud services and many other corporate actors, often described as intermediaries, promote, regulate or compromise privacy and expression online. Intermediaries may store massive volumes of user data, to which Governments often demand access. Encryption and anonymity may be promoted or compromised by each of these corporate actors.

28. A full exploration of the role of corporations to protect their users' security online is beyond the scope of the present report, which is focused on State obligations. However, it remains important to emphasize that "the responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations" (see A/HRC/27/37, para. 43). At a minimum, corporations should apply principles such as those laid out in the

[12] The European Court of Human Rights has recognized this point. See *Ahmet Yildirim* v. *Turkey*,(2012); *Cox* v. *Turkey*, (2010); *Case of Groppera Radio AG and Others* v. *Switzerland* (1990).

[13] European Commission of Human Rights, *Neij and Sunde Kolmisoppi* v. *Sweden*, (2013); European Court of Human Rights, *Perrin* v. *United Kingdom*, (2005); African Court on Human and Peoples' Rights, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Meldrum)* v. *Zimbabwe* (2009); *Case of Herrera Ulloa* v. *Costa Rica*, *Herrera Ulloa* v. *Costa Rica*, Preliminary Objections, Merits, Reparations and Costs, Series C No. 107, IHRL 1490 (IACHR 2004).

[14] See *Autronic AG* v. *Switzerland* (1990); *De Haes and Gijsels* v. *Belgium* (1997), para. 48; *News Verlags GmbH and Co.KG v. Austria* (2000).

Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights and the Telecommunications Industry Dialogue Guiding Principles, which encourage corporations to commit to protect human rights, undertake due diligence to ensure the positive human rights impact of their work and remediate adverse impacts of their work on human rights. In the future, the Special Rapporteur will focus on the roles corporations should play in preserving individual security to exercise freedom of opinion and expression.

IV. Evaluating restrictions on encryption and anonymity

A. Legal framework

29. The permissible limitations on the right to privacy should be read strictly, particularly in an age of pervasive online surveillance — whether passive or active, mass or targeted — regardless of whether the applicable standards are "unlawful and arbitrary" under article 17 of the International Covenant on Civil and Political Rights, "arbitrary" under article 12 of the Universal Declaration, "arbitrary or abusive" under article 11 of the American Convention on Human Rights, or "necessary in a democratic society" under article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (see A/HRC/13/37, paras. 14–19). Privacy interferences that limit the exercise of the freedoms of opinion and expression, such as those described in this report, must not in any event interfere with the right to hold opinions, and those that limit the freedom of expression must be provided by law and necessary and proportionate to achieve one of a handful of legitimate objectives.

30. No restrictions may be imposed on the right to hold opinions without interference; restrictions under article 19 (3) of the Covenant only apply to expression under article 19 (2). In environments where one's opinions, however held online, result in surveillance or harassment, encryption and anonymity may provide necessary privacy. Restrictions on such security tools may interfere with the ability of individuals to hold opinions.

31. Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.

32. First, for a restriction on encryption or anonymity to be "provided for by law", it must be precise, public and transparent, and avoid providing State authorities with unbounded discretion to apply the limitation (see Human Rights Committee, general comment No. 34 (2011)). Proposals to impose restrictions on encryption or anonymity should be subject to public comment and only be adopted, if at all, according to regular legislative process. Strong procedural and judicial safeguards should also be applied to guarantee the due process rights of any individual whose use of encryption or anonymity is subject to restriction. In particular, a court, tribunal or other independent adjudicatory body must supervise the application of the restriction.[15]

33. Second, limitations may only be justified to protect specified interests: rights or reputations of others; national security; public order; public health or morals. Even where a State prohibits by law " advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, as provided by Article 20 of the Covenant, any restrictions on expression must be consistent with Article 19(3) (A/67/357). No other grounds may justify restrictions on the freedom of expression. Moreover, because legitimate objectives are often cited as a pretext for illegitimate purposes, the restrictions themselves must be applied narrowly.[16]

34. Third, the State must show that any restriction on encryption or anonymity is "necessary" to achieve the legitimate objective.[17] The European Court of Human Rights has concluded appropriately that the word "necessary" in article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms means that the restriction must be

[15] See International Covenant on Civil and Political Rights, article 2 (3)(b); CCPR/C/79/Add.110, para. 22; the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

[16] See Human Rights Committee, general comment No. 34 on freedom of opinion and expression, para. 30, and general comment No. 31.

[17] See Human Rights Committee, general comment No. 34, para. 2, and communication No. 2156/2012, Views adopted on 10 October 2014.

something more than "useful," "reasonable" or "desirable".[18] Once the legitimate objective has been achieved, the restriction may no longer be applied. Given the fundamental rights at issue, limitations should be subject to independent and impartial judicial authority, in particular to preserve the due process rights of individuals.

35. Necessity also implies an assessment of the proportionality of the measures limiting the use of and access to security online.[19] A proportionality assessment should ensure that the restriction is "the least intrusive instrument amongst those which might achieve the desired result".[20] The limitation must target a specific objective and not unduly intrude upon other rights of targeted persons, and the interference with third parties' rights must be limited and justified in the light of the interest supported by the intrusion. The restriction must also be "proportionate to the interest to be protected".[21] A high risk of damage to a critical, legitimate State interest may justify limited intrusions on the freedom of expression. Conversely, where a restriction has a broad impact on individuals who pose no threat to a legitimate government interest, the State's burden to justify the restriction will be very high.[22] Moreover, a proportionality analysis must take into account the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter. In any case, "a detailed and evidence-based public justification" is critical to enable transparent public debate over restrictions that implicate and possibly undermine freedom of expression (see A/69/397, para. 12).

B. State practice: examples and concerns

36. The trend lines regarding security and privacy online are deeply worrying. States often fail to provide public justification to support restrictions. Encrypted and anonymous communications may frustrate law enforcement and counter-terrorism officials, and they complicate surveillance, but State authorities have not generally identified situations — even in general terms, given the potential need for confidentiality — where a restriction has been necessary to achieve a legitimate goal. States downplay the value of traditional non-digital tools in law enforcement and counter-terrorism efforts, including transnational cooperation.[23] As a consequence, the public lacks an opportunity to measure whether restrictions on their online security would be justified by any real gains in national security and crime prevention. Efforts to restrict encryption and anonymity also tend to be quick reactions to terrorism, even when the attackers themselves are not alleged to have used encryption or anonymity to plan or carry out an attack. Moreover, even where the restriction is arguably in pursuit of a legitimate interest, many laws and policies regularly do not meet the standards of necessity and proportionality and have broad, deleterious effects on the ability of all individuals to exercise freely their rights to privacy and freedom of opinion and expression.

37. It also bears noting that the United Nations itself has not provided strong communication security tools to its staff or to those who would visit United Nations websites, making it difficult for those under threat to securely reach the United Nations, human rights mechanisms online.[24]

1. Encryption

38. Some Governments seek to protect or promote encryption to ensure the privacy of communications. For instance,[25] the Marco Civil da Internet Law of Brazil, adopted in 2014, guarantees the inviolability and secrecy of user communications online, permitting exceptions only by court order. The E-Commerce Act and Telecommunication Act of Austria do not restrict encryption, and the Government has undertaken public awareness campaigns to educate the public about digital security. Greek law and regulations promote the effective use of both encryption and anonymity tools. Germany, Ireland and Norway permit and promote the use of encryption technologies and oppose any efforts to weaken encryption protocols. Similarly, Swedish and Slovak laws do not restrict the use of encryption online. The United States of

[18] See *Case of The Sunday Times* v. *United Kingdom*, judgement of 26 April 1979, para. 59.

[19] See African Court Human and Peoples' Rights, *Lohe Issa Konate* v. *Burkina Faso*, application No. 004/2013, paras. 148 and 149 (2014); European Court of Human Rights, *Case of The Sunday Times*, para. 62.

[20] See Human Rights Committee, general comment No. 27 (1999) on freedom of movement, para. 14.

[21] See ibid., para. 14.

[22] See Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134.

[23] But see Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).

[24] For instance, staff of the Office of the United Nations High Commissioner for Human Rights (OHCHR) in Geneva do not have access to end-to-end e-mail encryption, and the OHCHR website is not encrypted.

[25] Many examples in this paragraph are taken from the relevant government submissions.

America encourages the use of encryption, and the United States Congress should further consider a secure data act introduced in the Congress that would prohibit the Government from requiring companies to weaken product security or insert back-door access measures. Several Governments fund efforts to share or train in the use of encryption and anonymity technologies to help individuals evade censorship and protect their security online, including Canada, the Netherlands, Sweden, the United Kingdom of Great Britain and Northern Ireland and the United States. In addition, export regulations should facilitate the transfer of encryption technologies wherever possible. Although the present report does not provide an overall legal assessment of all national approaches to encryption, these noted elements — non-restriction or comprehensive protection, the requirement of court orders for any specific limitation, and public education — deserve wider application as means to protect and promote the rights to freedom of opinion and expression.

39. Nonetheless, the regulation of encryption often fails to meet freedom of expression standards in two leading respects. First, restrictions have generally not been shown to be necessary to meet a particular legitimate interest. This is especially the case given the breadth and depth of other tools, such as traditional policing and intelligence and transnational cooperation, that may already provide substantial information for specific law enforcement or other legitimate purposes. Second, they disproportionately impact the rights to freedom of opinion and expression enjoyed by targeted persons or the general population.

Bans on encryption for individual use

40. Outright prohibitions on the individual use of encryption technology disproportionately restrict the freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression, without any particular claim of the use of encryption for unlawful ends.

41. State regulation of encryption may be tantamount to a ban, such as rules (a) requiring licences for encryption use; (b) setting weak technical standards for encryption; and (c) controlling the import and export of encryption tools. By limiting encryption tools to government-approved standards and controlling the import or export of encryption technologies, States ensure encryption software maintains weaknesses that allow Governments to access the content of communications. For example, while the law may be in flux, India has provided that service providers may not deploy "bulk encryption" on their networks, while the law has also restricted individuals from using encryption greater than an easily breakable 40-bit key length without prior permission and required anyone using stronger encryption to provide the Government with a copy of the encryption keys.[26] Reports indicate that encryption products in China may be required to adhere to government-approved encryption algorithms that have not been peer-reviewed for security.[27] The Pakistan Telecommunication Authority requires prior approval for the use of VPNs and encryption.[28] Cuba requires regulatory authorization for those using encryption.[29] In Ethiopia, the Government has the power to set the technical standards of encryption and recently enacted regulation that criminalizes the manufacture, assembly or import of any telecommunications equipment without a permit.[30] Such regulations impermissibly interfere with the individual use of encryption in communications.

Intentional weakening of encryption

42. Some States have implemented or proposed implementing so-called back-door access in commercially available products, forcing developers to install weaknesses that allow government authorities access to encrypted communications. Some Governments have developed or purchased tools to allow such access for domestic surveillance purposes.[31] Senior officials in the United Kingdom and the United States appear to advocate requiring back-door access.[32] States supporting such measures often claim that a legal framework for back-door access is necessary to intercept the content of encrypted communications. Governments

[26] Government of India, Ministry of Communications and IT, Licence Agreement for Provision of Internet Services, (2007). Available from http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. See especially sect. 2.2 (vii).

[27] See, e.g., Counter-terrorism Law, art. 15 (initial draft of 8 November 2014). Available from http://chinalawtranslate.com/en/ctldraft/.

[28] See www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

[29] Submission of Cuba.

[30] See Ethiopia Telecom Fraud Offence Proclamation 761/2012, sects. 3–10.

[31] See Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

[32] See the speech given by Prime Minister David Cameron on 12 January 2015 at the Conservative Party pledges conference for the 2015 general election and the speech given by James Comey, Director of the Federal Bureau of Investigation, on 16 October 2014, entitled "Going dark: are technology, privacy and public safety on a collision course?", at the Brookings Institution, Washington, D.C.

19

proposing back-door access, however, have not demonstrated that criminal or terrorist use of encryption serves as an insuperable barrier to law enforcement objectives. Moreover, based on existing technology, intentional flaws invariably undermine the security of all users online, since a backdoor, even if intended solely for government access, can be accessed by unauthorized entities, including other States or non-State actors. Given its widespread and indiscriminate impact, back-door access would affect, disproportionately, all online users.

43. The debate on this issue highlights a critical point: requiring encryption back-door access, even if for legitimate purposes, threatens the privacy necessary to the unencumbered exercise of the right to freedom of expression. Back-door access has practical limitations; the exploitation of intentional weaknesses could render encrypted content susceptible to attack, even if access is provided with the sole intention of allowing government or judicial control. Governments certainly face a dilemma when their obligation to protect freedom of expression is in conflict with their obligations to prevent violations of the right to life or bodily integrity, which are put at risk by terrorism and other criminal behaviour. But other recourses are available to States to request the disclosure of encrypted information, such as through judicial warrants. In such situations, States must demonstrate that general limitations on the security provided by encryption would be necessary and proportionate. States must show, publicly and transparently, that other less intrusive means are unavailable or have failed and that only broadly intrusive measures, such as backdoors, would achieve the legitimate aim. Regardless, measures that impose generally applicable restrictions on massive numbers of persons, without a case-by-case assessment, would almost certainly fail to satisfy proportionality.

Key escrows

44. A key escrow system permits individual access to encryption but requires users to store their private keys with the Government or a "trusted third party". Key escrows, however, have substantial vulnerabilities. For instance, the key escrow system depends on the integrity of the person, department or system charged with safeguarding the private keys, and the key database itself could be vulnerable to attack, undermining any user's communication security and privacy. Key escrow systems, rejected (along with back-door access) after significant debate in the United States in the so-called Crypto Wars of the 1990s, are currently in place in several countries and have been proposed in others. In 2011, Turkey passed regulations requiring encryption suppliers to provide copies of encryption keys to government regulators before offering their encryption tools to users.[33] The vulnerabilities inherent in key escrows render them a serious threat to the security to exercise the freedom of expression.

Mandatory key disclosure versus targeted decryption orders

45. In a situation where law enforcement or national security arguments may justify requests for access to communications, authorities may see two options: order either decryption of particular communications or, because of a lack of confidence that a targeted party would comply with a decryption order, disclosure of the key necessary for decryption. Targeted decryption orders may be seen as more limited and less likely to raise proportionality concerns than key disclosure, focusing on specific communications rather than an individual's entire set of communications encrypted by a particular key. Key disclosure, by contrast, could expose private data well beyond what is required by the exigencies of a situation.[34] Moreover, key disclosure or decryption orders often force corporations to cooperate with Governments, creating serious challenges that implicate individual users online. Key disclosure exists by law in a number of European countries.[35] In both cases, however, such orders should be based on publicly accessible law, clearly limited in scope focused on a specific target, implemented under independent and impartial judicial authority, in particular to preserve the due process rights of targets, and only adopted when necessary and when less intrusive means of investigation are not available. Such measures may only be justified if used in targeting a specific user or users, subject to judicial oversight.

Legal presumptions

46. Some States may identify the mere use of encryption technologies as illicit behaviour. For instance, charges against the Zone 9 blogger collective in Ethiopia included suggestions

[33] Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting.

[34] The European Commission Counter-Terrorism Coordinator has urged consideration of mandatory key disclosure. See Council of the European Union, General Secretariat, meeting document D1035/15 (2015).

[35] See, e.g., United Kingdom, Regulation of Investigatory Powers Act (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure).

that the mere training in communication security was evidence of criminal behaviour.[36] Such presumptions fail to meet the standards for permissible restrictions. Similarly, States undermine the rights to privacy and freedom of expression when they penalize those who produce and distribute tools to facilitate online access for activists.

2. Anonymity

47. Anonymity has been recognized for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate.[37] The Universal Declaration and the International Covenant on Civil and Political Rights do not address anonymity. During negotiation of the Covenant, it was proposed to include in article 19 (1) the phrase, "anonymity is not permitted". However, this was rejected "on the grounds, among others, that anonymity might at times be necessary to protect the author" and "that such a clause might prevent the use of pen names".[38] The Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights found that "the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions".[39] Several States enjoy long traditions of celebrating anonymity in their political cultures, but very few provide general protection in law for anonymous expression. Some States exert significant pressure against anonymity, offline and online. Yet because anonymity facilitates opinion and expression in significant ways online, States should protect it and generally not restrict the technologies that provide it. Several States' judiciaries have protected anonymity, at least in limited instances. For instance, the Supreme Court of Canada recently struck down the warrantless acquisition of anonymous user identity online.[40] The Constitutional Court of the Republic of Korea struck down anti-anonymity laws as unconstitutional.[41] The Supreme Court of the United States has consistently protected the right to anonymous expression.[42] The European Court of Human Rights has recognized anonymity as important to the freedom of expression but permits limitations in cases where necessary to achieve legitimate objectives.

48. Many States recognize the lawfulness of maintaining the anonymity of journalists' sources. The Mexican Supreme Court and Mexican Code of Criminal Procedures recognize the right of journalists to maintain the anonymity of their sources; yet pressures on journalists are in fact severe.[43] The Constitutions of Argentina, Brazil, Ecuador and Paraguay explicitly protect sources; Chile, El Salvador, Panama, Peru, Uruguay and Venezuela (Bolivarian Republic of) protect sources in law.[44] The Mozambique Constitution protects sources, while Angola purports to do so by statute.[45] Australia, Canada, Japan and New Zealand have established case-specific judicial balancing tests to analyse source protection, although pressure on journalists may undermine such protections over time.[46] States often breach source anonymity in practice, even where it is provided for in law.

Prohibition of anonymity

49. Prohibition of anonymity online interferes with the right to freedom of expression. Many States ban it regardless of any specific government interest. The Constitution of Brazil (art. 5) prohibits anonymous speech. The Constitution of the Bolivarian Republic of Venezuela (art. 57) similarly prohibits anonymity. In 2013, Viet Nam outlawed the use of pseudonyms, which forced individuals with personal blogs to publicly list their real name and address.[47] In 2012, the

---

[36] See http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

[37] See, e.g., Inter-American Commission on Human Rights, OEA /Serv.L/V/II.149, para. 134; United States, *McIntyre* v. *Ohio Elections Commission* (1995); Lord Neuberger, speech to RB Conference on the Internet, entitled, "What's a name? Privacy and Anonymous Speech on the Internet" (2014).

[38] Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (1987), pp. 379-80.

[39] See Organization of American States, press release 17/15.

[40] *R.* v. *Spencer* (2014).

[41] Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.

[42] *McIntyre* v. *Ohio Elections Commission* (1995), pp. 342 and 343.

[43] See new Federal Code of Criminal Procedures, art. 244.

[44] See Argentina, Constitution, art. 43; Brazil, Constitution, title II, chap. I, art. 5, XIV; Ecuador, Constitution, art. 20; Paraguay, Constitution, art. 29 (1). See also Chile, Law 19,733; El Salvador, Criminal Procedure Code; Panama, Law 67, art. 21; Peru, Criminal Procedure Code; Uruguay, Law 16.099; Bolivarian Republic of Venezuela, Law for Journalism 4.819, art. 8.

[45] See Mozambique, Constitution, art. 48(3); Angola, Press Law 7/06, art. 20(1).

[46] Australia Evidence Amendment (Journalists' Privilege) Act 2007; Canada, Court of Queen's Bench of Alberta, *Wasylyshen* v. *Canadian Broadcasting Corporation* (2005); Japan, Case 2006 (Kyo) No. 19 (2006); New Zealand Evidence Act, sect. 68 (2006).

[47] Human Rights Watch, "Vietnam: new decree punishes press", 23 February, 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19, Comment on Decree No. 02 of 2011 on Administrative

Islamic Republic of Iran required the registration of all IP addresses in use inside the country and cybercafe users to register their real names before using a computer.[48] Ecuadoran law requires commenters on websites and mobile phone owners to register under a real name.[49]

50. Certain States have passed laws that require real-name registration for online activity, a kind of ban on anonymity. In the Russian Federation, bloggers with 3,000 or more daily readers must register with the media regulator and identify themselves publicly, and cybercafe users reportedly must provide identification to connect to public wireless facilities.[50] China reportedly announced regulations requiring Internet users to register real names for certain websites and avoid spreading content that challenges national interests.[51] South Africa also requires real name registration for online and mobile telephone users.[52]

51. Likewise, Governments often require SIM card registration; for instance, nearly 50 countries in Africa require or are in the process of requiring the registration of personally identifiable data when activating a SIM card.[53] Colombia has had a mandatory mobile registration policy since 2011, and Peru has associated all SIM cards with a national identification number since 2010.[54] Other countries are considering such policies. Such policies directly undermine anonymity, particularly for those who access the Internet only through mobile technology. Compulsory SIM card registration may provide Governments with the capacity to monitor individuals and journalists well beyond any legitimate government interest.

52. States have also attempted to combat anonymity tools, such as Tor, proxies and VPNs, by denying access to them. China has long blocked access to Tor,[55] and Russian government officials reportedly offered more than $100,000 for techniques to identify anonymous users of Tor.[56] In addition, Ethiopia,[57] Iran (Islamic Republic of)[58] and Kazakhstan[59] have reportedly sought to block Tor traffic. Because such tools may be the only mechanisms for individuals to exercise freedom of opinion and expression securely, access to them should be protected and promoted.

Restrictions during public unrest

53. Anonymous speech has been necessary for activists and protestors, but States have regularly attempted to ban or intercept anonymous communications in times of protest. Such attempts to interfere with the freedom of expression unlawfully pursue an illegitimate objective of undermining the right to peaceful protest under the Universal Declaration and the International Covenant on Civil and Political Rights.

Intermediary liability

54. Some States and regional courts have moved towards imposing responsibilities on Internet service providers and media platforms to regulate online comments by anonymous users. Ecuador, for instance, in its Organic Communications Law, requires intermediaries to generate mechanisms to record personal data to allow the identification of those posting comments. In *Delfi* v. *Estonia* (application No. 64569/09), the European Court of Human Rights upheld an Estonian law that imposes liability on a media platform for anonymous defamatory statements posted on its site. Such intermediary liability is likely to result either in real-name registration policies, thereby undermining anonymity, or the elimination of posting

Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam (June 2011).

48 Islamic Republic of Iran, Bill 106, Communication Regulation Authority.

49 See Ecuador, Organic Law on Communications (2013).

50 Bill No. 428884-6 amending the Federal Law on Information, Information Technologies and Protection of Information and a number of legislative acts of the Russian Federation on streamlining the exchange of information with the use of information and telecommunication networks; Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi," 8 August 2014.

51 China Copyright and Media, Internet User Account Name Management Regulations, article 5 (2015).

52 South Africa, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2003; see also Electronic Communications and Transactions Act of 2002 (requiring real name registration for service providers).

53 Kevin P. Donovan and Aaron K. Martin, "The Rise of African SIM Registration", 3 February 2014.

54 See Colombia, Decree 1630 of 2011; Perú 21, *Los celulares de prepago en la mira*, 27 May 2010.

55 MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 April 2012.

56 The original offer is available from http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008.

57 Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012); see also Article 19, 12 January 2015.

58 "Phobos", "Iran partially blocks encrypted network traffic", The Tor Blog (10 February 2012).

59 "Phobos", "Kazakhstan upgrades censorship to deep packet inspection", The Tor Blog (16 February 2012).

altogether by those websites that cannot afford to implement screening procedures, thus harming smaller, independent media. The recently adopted Manila Principles on Intermediary Liability, drafted by a coalition of civil society organizations, provide a sound set of guidelines for States and international and regional mechanisms to protect expression online.

Data retention

55. Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint. A State's ability to collect and retain personal records expands its capacity to conduct surveillance and increases the potential for theft and disclosure of individual information.

V. Conclusions and recommendations

56. Encryption and anonymity, and the security concepts behind them, provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age. Such security may be essential for the exercise of other rights, including economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity. Because of their importance to the rights to freedom of opinion and expression, restrictions on encryption and anonymity must be strictly limited according to principles of legality, necessity, proportionality and legitimacy in objective. The Special Rapporteur therefore recommends the following.

A. States

57. States should revise or establish, as appropriate, national laws and regulations to promote and protect the rights to privacy and freedom of opinion and expression. With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education.

58. Discussions of encryption and anonymity have all too often focused only on their potential use for criminal purposes in times of terrorism. But emergency situations do not relieve States of the obligation to ensure respect for international human rights law. Legislative proposals for the revision or adoption of restrictions on individual security online should be subject to public debate and adopted according to regular, public, informed and transparent legislative process. States must promote effective participation of a wide variety of civil society actors and minority groups in such debate and processes and avoid adopting such legislation under accelerated legislative procedures. General debate should highlight the protection that encryption and anonymity provide, especially to the groups most at risk of unlawful interferences. Any such debate must also take into account that restrictions are subject to strict tests: if they interfere with the right to hold opinions, restrictions must not be adopted. Restrictions on privacy that limit freedom of expression — for purposes of the present report, restrictions on encryption and anonymity — must be provided by law and be necessary and proportionate to achieve one of a small number of legitimate objectives.

59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.

60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows. In addition, States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users. Corporate actors should likewise consider their own policies that restrict encryption and anonymity (including through the use of pseudonyms). Court-ordered decryption, subject to domestic and international law, may only be permissible when it results from transparent and publicly accessible laws applied solely on a targeted,

case-by-case basis to individuals (i.e., not to a mass of people) and subject to judicial warrant and the protection of due process rights of individuals.

B. International organizations, private sector and civil society

61. **States, international organizations, corporations and civil society groups should promote online security. Given the relevance of new communication technologies in the promotion of human rights and development, all those involved should systematically promote access to encryption and anonymity without discrimination. The Special Rapporteur urgently calls upon entities of the United Nations system, especially those involved in human rights and humanitarian protection, to support the use of communication security tools in order to ensure that those who interact with them may do so securely. United Nations entities must revise their communication practices and tools and invest resources in enhancing security and confidentiality for the multiple stakeholders interacting with the Organization through digital communications. Particular attention must be paid by human rights protection mechanisms when requesting and managing information received from civil society and witnesses and victims of human rights violations.**

62. **While the present report does not draw conclusions about corporate responsibilities for communication security, it is nonetheless clear that, given the threats to freedom of expression online, corporate actors should review the adequacy of their practices with regard to human right norms. At a minimum, companies should adhere to principles such as those laid out in the Guiding Principles on Business and Human Rights, the Global Network Initiative's Principles on Freedom of Expression and Privacy, the European Commission's ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights, and the Telecommunications Industry Dialogue Guiding Principles. Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers.**

63. **The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world and, where necessary, to ensure that users at risk be provided the tools to exercise their right to freedom of opinion and expression securely.**

HIGH COURT OF MADRAS

(Special Original Jurisdiction)

WP. Nos. 20774 & 20214/2018

TYPED SET OF DOCUMENTS FILED

ON BEHALF OF THE INTERVENOR

VOLUME - II

M/S. ARUN KARTHIK MOHAN

(2110/2007)

SUHRITH PARTHASARATHY

(1133/2008)

COUNSEL FOR PETITIONER

MOBILE: 9884113886