IN THE HIGH COURT OF JUDICATURE AT MADRAS

(Special Original Jurisdiction)

W.P. 20774 & 20214 of 2019

Internet Freedom Foundation (IFF)
A registered charitable trust through its
Executive Director, Mr. Apar Gupta
E-215, Third Floor, East of Kailash
New Delhi – 110065 ... Intervenor

Versus

Antony Clement Rubin ... Respondent/Petitioner
[in W.P No. 20774 of 2019]

Union of India & Others
...Respondents/Respondents

And

Janani Krishnamurthy ... Respondent/Petitioner
[in W.P No. 20214 of 2019]

Union of India & Others
...Respondents/Respondents

AFFIDAVIT FILED ON BEHALF OF THE INTERVENOR TRUST IN RESPONSE TO REPORT OF PROF. V. KAMAKOTI DATED 31.07.2019

I, Apar Gupta, Executive Director of the Internet Freedom Foundation aged about 35 years, having an office at E-215, Third Floor, East of Kailash, New Delhi-110065, do hereby solemnly affirm and sincerely state as follows:

1. I am the Executive Director of the Intervenor Trust, and as such, I am well acquainted with the facts of the case. I am authorized and competent to swear this affidavit for and on behalf of the Intervenor Trust.

2. The Intervenor Trust is a charitable entity registered under the provisions of the Indian Trust Act, 1882, and it is a non-profit organization registered under Section 80G of the Income Tax Act, 1961. Vide order dated 27.06.2019, the Intervenor Trust was granted permission to intervene in W.P. 20774 & 20214 of 2019. Vide this Hon'ble Court's order dated 24.07.2019, Dr. V. Kamakoti, Professor at Indian Institute of Technology, Madras was directed to submit his technical opinion on traceability of the originator of messages on encrypted platforms such as WhatsApp. Pursuant to this Hon'ble Court's

AparGupta

direction, Dr. Kamakoti submitted his technical opinion titled 'Report on Originator traceability in WhatsApp messages' on 31.07.2019. Through this submission, the Intervenor Trust intends to respond to Dr. Kamakoti's report dated 31.07.2019, and with the permission of this Hon'ble Court, raise concerns about the proposal's impact on fundamental rights and also its technical feasibility and effectiveness.

Impact of Dr. Kamakoti's proposal on Fundamental Rights

3. In his report dated 31.07.2019, Dr. Kamakoti has proposed two methods of tracing the originator of a message sent through WhatsApp.

    - Through the first method, every receiver of a forwarded message will know the originator of the message as the originator's information is encrypted and forwarded along with the content of the message and every receiver can decrypt the content of the message as well as the originator's information.
    - Through the second method, the originator's information will be encrypted using a special public key and corresponding private key necessary to decrypt the originator's information will only be known to WhatsApp. Therefore, receivers of the message will only have access to the originator's information in an encrypted form and they will be unable to decrypt it because they do not have the corresponding private key which is held in escrow by WhatsApp. In case of commission of an offence, law enforcement agencies can request WhatsApp to decrypt the originator's information using the corresponding private key and trace the perpetrator.

4. In its reply dated 19.07.2019, the Intervenor Trust has highlighted various concerns associated with the first method suggested by Dr. Kamakoti and these concerns are being briefly restated for the convenience of this Hon'ble Court. First, this proposal puts individuals holding unpopular or dissenting viewpoints at risk of being subjected to violence or harassment by the majority because their identity will be known to every recipient of the message. Second, it will have a disproportionate impact on whistleblowers, activists, journalists, abuse survivors and marginalized groups because these categories of individuals are at greatest risk of harm if their identity was publicly disclosed. We respectfully restate these submissions and crave leave of this Hon'ble Court to refer to the contents of the reply dated 19.07.2019 filed by the Intervenor Trust.

Technical Feasibility and Effectiveness of Dr. Kamakoti's proposal

5. In order to evaluate the technical feasibility and effectiveness of Dr. Kamakoti's proposal, the Intervenor Trust sought assistance independently from Dr. Manoj Prabhakaran who is a Professor of Computer Science at the Indian Institute of

AparGupta

Technology, Bombay. Dr. Prabhakaran specializes in the field of cryptography and he has written extensively on the subject. We submit that we have sought his technical opinion completely independent of our reply dated 19.07.2019, and we have not suggested any changes to Dr. Prabhakaran's analysis. We further submit that such technical opinion has been sought and provided completely *gratis* without any consideration, influence or prior association but with the sole intent of rendering assistance to this Hon'ble Court.

6. In his response to Dr. Kamakoti's report dated 31.07.2019, Dr. Prabhakaran has highlighted certain vulnerabilities in the current proposal which enable falsification of originator information. Dr. Prabhakaran has also suggested techniques to mitigate the risk of spoofing of originator information but his analysis ultimately concludes that "*the effectiveness of the proposed mechanism (with or without the suggested modifications) is likely to be very limited.*" A true copy of Dr. Prabhakaran's technical opinion on Dr. Kamakoti's proposal for originator tracing in WhatsApp sent to the Intervenor-Trust via email dated 20.08.2019 is annexed herewith as **Annexure A**.

7. The Intervenor Trust has qualified technologists as members of its Board of Trustees, and it has also sought their views on the feasibility and effectiveness of Dr. Kamakoti's proposal. Based on the inputs received from Dr. Prabhakaran and other technical experts on its Board of Trustees, the Intervenor Trust respectfully submits that within the framework proposed by Dr. Kamakoti, bad actors can falsely modify the originator information to frame an innocent person for sending illegal messages. In his response, Dr. Prabhakaran has suggested using digital signatures to mitigate this risk. However, as he himself notes, even digital signatures cannot guarantee the accuracy of originator information in cases where the user's signing keys are stolen through malware, their one-time password is compromised or if the attacker has access to the SMS network.

8. The second method suggested by Dr. Kamakoti also relies on WhatsApp acting as a key escrow agent and decryption of originator information will require WhatsApp's cooperation. However, as noted by David Kaye, the UN Special Rapporteur on Freedom of Expression, in his Report on Encryption, Anonymity and the Human Rights Framework (UN Doc A/HRC/29/32), the security of the key escrow system depends on the integrity of the entity entrusted with safeguarding the key. Further, the key database itself could be vulnerable to hacking, thereby undermining the privacy and security of all users. In his response, Dr. Prabhakaran has also noted that if WhatsApp is the only watchdog who must cooperate for decryption of originator information, then the company may be placed under undue pressure by certain governments. A true copy of

NOTARY GOVT. OF INDIA
AJAY SETH
ADVOCATE

Apar Gupta

the UN Special Rapporteur's Report on Encryption, Anonymity and the Human Rights Framework (UN Doc A/HRC/29/32) is annexed herewith as **Annexure B.**

Need for proportionate solutions through policy processes

9. The Intervenor Trust respectfully submits that any proposal to change the design of an encrypted platform like WhatsApp would be highly technical and complex in nature. It is respectfully submitted that such a hyper factual, expert determination would require a deliberative policy formation process. This Hon'ble Court may avoid venturing into such a policy thicket given that recommending and enforcing changes to platform design would require extensive consultation with experts and other stakeholders, and it is humbly submitted that these functions are more suited for a regulatory or government authority such as the Ministry of Electronics and Information Technology. Such decisions by Government authorities may also be subject to further judicial review.

10. Finally, while the Petitioners' concerns about misuse of technology for illegal activities may arise in several instances, less restrictive alternatives may be more effective at combating some of these problems. For instance, we may counter fake viral incendiary messages through fact checking and awareness programmes. This has also been noted by Dr. Prabhakaran in his report where he states that *"there is increasing recognition that a lasting defence against the spread of fake news should be based on education and information literacy."* In view of the same, we restate our submissions as contained in the reply dated 19.07.2019 and respectfully request this Hon'ble Court to defer this technical and complex determination regarding encryption to a deliberative policy formulation body which through appropriate governmental processes can organise a consultation with transparency and public participation.

I identify the deponent / Executant / persons / parties, who has / have signed / put thumb impression in my presence

Solemnly affirmed at

BEFORE ME,

New Delhi on 20 August, 2019,

and signed in my presence

ADVOCATE,

NOTARY GOVT. OF INDIA AJAY SETH ADVOCATE Regn. No. 10669

ATTESTED NOTARY PUBLIC DELHI (INDIA)

20 AUG 2019

Entry in Notary Register No. 518

IN THE HIGH COURT OF
JUDICATURE AT MADRAS
(SPECIAL ORIGINAL JURISDICTION)
W.P. No. 20774 of 2019
20214

AFFIDAVIT FILED ON BEHALF
OF R15

MR. ARUN KARTHIK MOHAN
(2110/2007)
MR. SUHRITH PARTHASARATHY
(1133/2008)

COUNSEL FOR THE ~~PETITIONER~~ INTERVENOR/R 15