

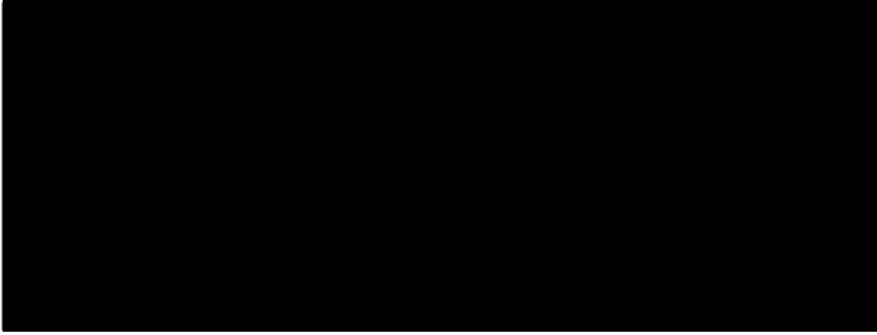
IN THE SUPREME COURT OF INDIA
CRIMINAL ORIGINAL JURISDICTION
PUBLIC INTEREST LITIGATION

WRIT PETITION (CRIMINAL) NO. 395 OF 2022

(Under Article 32 of the Constitution of India)

IN THE MATTER OF:-

Foundation for Media Professionals
Through its President.



...Petitioner

1. Union of India
Through Ministry of Home Affairs
North Block, Central Secretariat,
New Delhi - 110001
Through its Secretary ...Respondent No. 1
2. Ministry of Law and Justice
4th Floor, A-Wing,
Shastri Bhawan
New Delhi - 110001
Through its Secretary ...Respondent No. 2
3. Ministry of Finance
North Block, Central Secretariat,
New Delhi - 110001
Through its Secretary ...Respondent No. 3

A PETITION UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA PRAYING FOR AN APPROPRIATE WRIT OR DIRECTION FOR INTER ALIA GUIDELINES ON PRODUCTION, SEARCH, AND SEIZURE OF CONTENTS OF DIGITAL DEVICES

To

The Hon'ble Chief Justice of India
And His Companion Justices of the
Supreme Court of India.

The Humble Petition on behalf of
of the Petitioner above named.

MOST RESPECTFULLY SHOWETH:

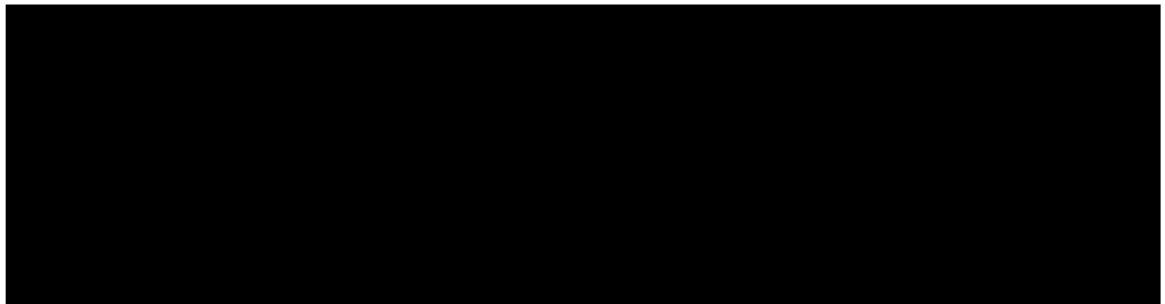
1. The present writ petition under Article 32 of the Constitution of India, filed in public interest, impugns the prevailing practices of various law enforcement agencies and other state agencies, which seek untrammelled access to digital devices of individuals. State agencies seek to justify these practices by invoking their powers to compel production of items, or conduct search and seizure operations during inquiries or investigations. Petitioners submit that these practices are contrary to, *inter alia*, the fundamental right to privacy inherent in Article 21 of the Constitution, other constitutional provisions, and as recognised by a Constitution Bench of this Hon'ble Court in *Justice (Retd.) K.S. Puttaswamy v. Union of India & Ors.* [(2017) 10 SCC 1]. Consequently, the present petition further prays for this Hon'ble Court to issue necessary directions and / or guidelines in respect of the exercise of these broad powers of law enforcement agencies, in order to adequately safeguard the right to privacy of persons.

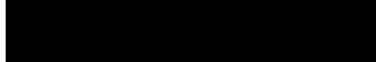
2. It is submitted that today, digital devices, especially personal devices such as mobile phones and laptops, contain more sensitive personal data about individuals than any physical space, such as a house or a vault. They can be found with a person almost at all times, and are effectively an extension of the self. Even if it is assumed that the existing legal provisions across general and special laws are applicable in context of the digital realm—going beyond mere production / seizure of devices but to the production / searches of their contents—it is submitted that existing legal provisions, either under the Criminal Procedure Code 1973 [Cr.P.C.] or under various special laws, are insufficiently tailored to ensure that law enforcement agencies exercise powers in a manner consistent with the fundamental right to privacy.
3. Law enforcement agencies have increasingly focused on personal digital devices precisely because of how integral these devices have become to a person's very existence. Compelling arrested persons to divulge passcodes of a digital device in order to gain real-time access to every facet of her life, in a manner wholly contrary to Articles 20(3) and 21 of the Constitution, has become the norm for investigations. In various parts of the country police have assumed powers to compel any random passerby to unlock his mobile phone and share its contents, with no prior judicial warrant or notice let alone any semblance of a fair trial, causing persons to waive their fundamental rights altogether out of fear. And material that is accessed by agencies from such digital devices has been known to find its way into the hands of media agencies which use the same to irrevocably damage a person's reputation.

4. In the absence of both a statutory framework which is in consonance with the concepts of human dignity and individual autonomy guaranteed by the Constitution, and the absence of any judicial decision by this Hon'ble Court on these issues, individuals have been rendered helpless and without any protection against intrusion by the state into the deepest recesses of her personal life by law enforcement agencies purportedly pursuing inquiries or investigations. These consequences are all the more serious for journalists, some of whom the Petitioner Society represents, owing to the heavy reliance they place on digital devices for their profession. These unchecked powers of the state, often targeted against journalists and their privacy, are actively spreading a deleterious chilling effect in society and urgently require judicial tempering by this Hon'ble Court.

DESCRIPTION OF PARTIES

5.



 The Petitioner-Society is engaged *inter alia* in activities to expand the freedom of the media, and to provide inputs on legislation on matters affecting the news media either directly or indirectly, and to make appropriate representations to Parliament and other institutions and organisations at all levels of government and public life. The Petitioner-Society's founding members include eminent journalists namely, Amitabh Thakur, Aniruddha Bahal, Ashutosh, Madhu Trehan, Manoj Mitta, S. Srinivasan, Sanjay Pugalia, Sanjay Salil, Shashi Shekhar, Vineet Narain and Vivian Fernandes. A true copy of the

registration certificate of the Petitioner Society bearing Registration [REDACTED] is annexed herewith as ANNEXURE P-1(104). A true copy of the Memorandum of Association and rules and regulations of the Petitioner-Society is annexed herewith as ANNEXURE P-2(105-127). A true copy of the Petitioner's PAN Card is Annexed herewith as ANNEXURE P-3(128-129).

6. The governing body of the Petitioner-Society as on date has the following composition:
 - a. President: Samrat Choudhury
 - b. Director: Raksha Kumar
 - c. Governing Body Members: Aniruddha Bahal, Manoj Mitta, Paranjoy Guha Thakurta, S Srinivasan, Nitin Sethi, Vipul Mudgal, Vivian Fernandes.

7. The Petitioner-Society was established to protect journalists and advance freedom of the press, and it has responsibly engaged with the government and the Hon'ble Courts on this issue. Some instances are detailed below:
 - a. The Petitioner-Society had previously filed W.P. (Crl) No. 106 of 2015 titled *Foundation of Media Professionals v. Union of India* [(2015) 9 SCC 252] before this Hon'ble Court challenging the criminalisation of defamation through Sections 499 and 500 of the Indian Penal Code, 1860 and Sections 199(1) and 199(2) of the Code of Criminal Procedure, 1973 as being contrary to the fundamental rights of journalists under Articles 14, 19 and 21 of the Constitution of India. This Petition culminated in the judgment dated April 7, 2015 in *Subramanian Swamy v. Union of India* (2015) 13 SCC 356.

- b. The Petitioner-Society filed an Application for Intervention / Impleadment, IA No. 139555/2019 in W.P. (C) No. 1031 / 2019 titled '*Anuradha Bhasin v. Union of India*', which was taken on record by this Hon'ble Court *vide* order dated 01.10.2019, granting liberty to the Petitioner-Society to file additional documents in support of its Application. In the judgment and final order, reported as *Anuradha Bhasin v. Union of India & Ors* [(2020) SCC Online SC 25], this Hon'ble Court was pleased to take note and consider the submissions of the Counsel for the Petitioner-Society.
- c. The Petitioner also spearheaded the restoration of internet services in Jammu & Kashmir in 2020 in *Foundation of Media Professionals v. State (UT of J&K* [(2020) 5 SCC 746].
- d. The Petitioner was heard by a Constitution Bench of this Hon'ble Court as an intervenor in *Sahara India Real Estate Corp. Ltd. v. Securities & Exchange Board of India* [(2012) 10 SCC 603], also known as the 'Media Guidelines Case'.
- e. The Petitioner has also challenged the constitutionality of Section 124-A of the Indian Penal Code, 1860 [Sedition] by filing an Intervention Application, being I.A. No. 78477 in Writ Petition (Criminal) No. 106 of 2021, titled *Kishorechandra Wangkhemcha & Anr. v. Union of India*, which is pending before this Hon'ble Court.
8. The Petitioner-Society does not have any personal interest or any personal gain or private motive or any other oblique reason in filing this Writ Petition in Public Interest.

9. The Petitioner-Society has not been involved in any other civil or criminal or revenue litigation, which could have legal nexus with the issues involved in the present Petition.

THE EXISTING INDIAN LEGAL REGIME GOVERNING COMPELLED PRODUCTION OF DOCUMENTS OR THINGS

10. In respect of arrested persons, police and other law enforcement agencies retain powers under Section 51, Cr.P.C. to carry out searches upon arrest, and seize personal effects that may be found as a result. For all other cases, agencies must resort to their powers to compel production of things, and of search and seizure. These powers vested in law enforcement agencies are spread across various statutory provisions in India. The general provisions conferring such powers upon agencies are contained within Chapter VIII of the Cr.P.C., 1973 and are briefly described hereunder:

- i. Section 91 empowers the police or a competent court to issue a written order or summons, respectively, to a person for producing a 'document' or 'thing'. It must be demonstrated that such a document or thing is 'necessary' or 'desirable' for purposes of any investigation, inquiry, trial or other proceeding under the Cr.P.C [Section 91(1)]. 'Document', is defined under Section 29 of the Indian Penal Code, 1860 [IPC], and it does not include electronic records.
- ii. Section 92 specifically covers issuing notices in respect of documents or things in the custody of postal authorities; notably, it does not confer upon the police any powers to compel production of such items. Instead it only confers a power upon courts to issue necessary directions to postal authorities, where the production of items is "*necessary for the purpose of any inquiry, investigation, or trial*" under the Code.

- 8
- iii. Section 93 provides for issuance of a search warrant of 'places' by a court in three circumstances: (i) when the court believes that a person to whom summons has been issued under Section 91 will not produce the required document or thing [93(1)(a)]; (ii) where such document or thing is not known to the court to be in the possession of any person [93(1)(b)], or; (iii) when the court considers that a general search or inspection is required for any inquiry, trial or other proceeding [93(1)(c)]. A court may, whilst issuing warrants, specify the place or part thereof to which a search or inspection shall extend [93(2)].
 - iv. Section 94 provides for issuance of a warrant for the search of a place for any stolen property or any other 'objectionable article' as defined under Section 94(2). It does not include digital devices.
 - v. Section 100 provides the procedure for search of closed places. "Place" is defined under Section 2(p), Cr.P.C. to include a house, building, tent, vehicle and vessel. A person residing in or in charge of such a place is mandated to allow its search or inspection, even if it is a closed place, upon production of a warrant. The provision also permits search of a person in or around the closed place, who is suspected of concealing an article for which search is authorised. The person must allow free entry into the closed place and provide 'all reasonable facilities' for a search. Certain procedural safeguards have been incorporated in Section 100, such as: (i) requiring two or more witnesses be present during search, (ii) preparing a list of items seized along with the place they are found, and (iii) permitting the occupant of the closed place to attend searches and retain a copy of the list of items so prepared.
 - vi. Section 102 grants police a power to seize property in two situations: (i) when property may be alleged or suspected of being stolen, or (ii)

when it is found under circumstances which create suspicion of commission of any offence.

- vii. Section 103 grants very wide powers to a Magistrate to direct search of any place at his discretion. Such a place, however, can only be a place for which the Magistrate is competent to issue a search-warrant.
11. At the same time, Section 165, Cr.P.C. provides wide powers of conducting warrantless searches of 'places' to police officers. A warrantless search under this provision is exceptional and can only be carried out in situations of urgency when a police officer has reasonable grounds to believe that (i) anything necessary for an investigation may be found in a place within the jurisdiction of the concerned police station, and (ii) such thing cannot be obtained without undue delay without the warrantless search. These twin conditions are both mandatory, and police officers conducting a warrantless search must record reasonable grounds of her belief in writing, and identify (as far as possible) the thing for which search is to be made.
12. The gist of the general scheme, therefore, is that documents or things can be secured either by a person willingly complying with a request to provide the same (crucially, with the legal definition of 'document' not inclusive of 'electronic records', and with limitations upon material in possession of postal and telegraph authorities). Or, the police agencies can intrude into a person's privacy by carrying out search and seizure operations of 'places' to secure the same (but the term 'place' is defined to only cover a 'house, building, tent, vehicle and vessel' in the statute). While the general scheme contains a requirement for police to obtain warrants prior to carrying out an intrusive action, this is subject to broad exceptions enabling exercise of such powers without warrant when facing

specified exigencies. Crucially though, the exception for police to carry out warrantless searches does not extend to carrying out a general search as under Section 93(1)(c), Cr.P.C. but for searches *qua* a specific document or thing akin to Section 93(1)(a).

13. These general powers to secure documents or things co-exist with specific provisions set out in various other statutes, such as:
 - a. Section 42 of the Narcotic Drugs & Psychotropic Substances Act, 1985 provides for warrantless entry, search, seizure, and arrest. Persons authorised under the provision can enter into and search any 'building, conveyance or place' between sunrise and sunset if they believe that - (i) any narcotic drug, psychotropic substance, controlled substance, (ii) any document or article which may be used as evidence in the commission of any offence under the Act or (iii) any illegally acquired property, document or article which may be used as evidence of holding any illegally acquired property liable for seizure or freezing or forfeiture under the Act, is kept or concealed in any such building, conveyance or enclosed place.
 - b. Sections 17 and 18 of the Prevention of Money Laundering Act, 2002 provide for search and seizure. Section 17 empowers certain officials to 'enter and search any building, place, vessel, vehicle or aircraft' if the official has reasons to believe that any person has (i) committed any act which constitutes money-laundering, or (ii) is in possession of any proceeds of crime involved in money-laundering, or (iii) is in possession of any records relating to money-laundering, or (iv) is in possession of any property related to crime, and such record or proceeds are kept there. Section 18 of that Act sets similar conditions for a warrantless search of one's person.

- c. Sections 100 to 103 of the Customs Act, 1962 provide specifically for the *search of persons* if any person is found to have secreted about her person any goods mentioned under Section 101 that are liable to confiscation, or documents relating thereto.
- d. Section 132 of the Income Tax Act, 1961 allows search and seizure by “entering and searching any building, place, vessel, vehicle or aircraft” where the person authorised has reasons to suspect that certain books of account, other documents, money, bullion, jewellery or other valuable articles or things are kept. The provision also allows *search of persons* who have got out of, or are about to get into, or are in such a building, place, vessel, vehicle or aircraft. Section 133A of the Income Tax Act, 1961 grants wide powers for authorities to enter certain *places* defined under the section for the purpose of (i) inspecting such books of account or other documents as may be required and which may be available at such place, (ii) checking or verify the cash, stock or other valuable article or thing which may be found therein, and (iii) for furnishing such information as may be required for any matter which may be useful or relevant to any proceeding under the Income Tax Act. Despite the provision of survey being limited to *places*, the provision is used to search and seize electronic devices.
- e. Sections 217 and 220 of the Companies Act, 2013 give the power to Inspectors under that act to demand furnishing of books or papers pertaining to the affairs of companies or persons whose affairs are being investigated, and seizure of such materials, respectively.
- f. Section 41 of the Competition Act, 2002, confers upon the Director General appointed under that Act powers that are otherwise available to Inspectors under Sections 240 and 240A of the

erstwhile Companies Act, 1956 — provisions that are *in pari materia* with Sections 217 and 220 of the Companies Act, 2013.

- g. Section 67 of the Central Goods and Services Act, 2017 provides for inspection, search and seizure of certain places, goods, documents, books or things. The places include places of business of the taxable person or persons engaged in the business of transporting goods or the owner or operator of warehouse or godown or any other place - in cases where such persons have suppressed any transaction relating to supply of goods or services or both or the stock of goods in hand, or have claimed input tax credit in excess of their entitlement under the Act or have indulged in contravention of any of the provisions of the Act to evade tax, or are keeping goods which have escaped payment of tax or have kept their accounts or goods in such a manner as is likely to cause evasion of tax payable under the Act.

These provisions under special laws broadly follow the scheme of the general law. If anything, they further reduce the requirement for obtaining prior warrants for search actions. Pertinently, none of the provisions on search and seizure under special laws makes specific reference to either digital devices or electronic records.

14. The general law found in the Cr.P.C. 1973, which forms the basis for the legal regime found across various special laws, has been adopted without any significant alteration from the original scheme provided by the colonial administrators under the Codes of Criminal Procedure of 1872 and 1882. It is an almost exact reproduction of the scheme as it existed in the erstwhile Code of Criminal Procedure, 1898. Contemporaneous speeches of legislators suggest that these provisions were drafted with the

assumption that the subjects of the law bore no liberty interests which the law had to protect [See, speech of the then Lieutenant-Governor of Bengal in the proceedings of the Legislative Council on the Criminal Procedure Bill of 1872, excerpted in *Ahmed Mahomed Jackariah v. Ahmed Mahomed*, (1888) ILR 15 Cal 109].

15. It is trite that this logic of colonial governance today stands fundamentally transformed by virtue of India's independence and the recognition of each citizen's individual autonomy and dignity, which are guaranteed by a set of fundamental rights found in the Constitution. These rights and interests of Indian citizens form the cornerstone of India's democracy, and are now placed at the heart of a Constitution that guarantees the right to life and personal liberty [Art. 21], the right to freedom of speech and expression [Art. 19(1)(a)], to assemble peaceably [Art. 19(1)(b)], to form associations [Art. 19(1)(c)], to move freely throughout the territory of India [Art. 19(1)(d)], to practise any profession, occupation, trade or business [Art. 19(1)(g)], the right against self incrimination for accused persons [Art 20(3)], and provides protection against arrest and detention [Art. 22]. Recognition of individual liberties, the right to live with dignity and the right to privacy under Articles 14, 19, and 21, acts as a source of restraint against unreasonable state action.
16. In spite of these transformative changes witnessed in the fabric of the Indian legal system witnessed during the century between 1872 to 1973, no alterations were somehow made to the Cr.P.C. provisions which had a direct impact on personal liberty, dignity, and privacy. Nevertheless, this Hon'ble Court has unwaveringly stepped in to secure respect for these basic values guaranteed by fundamental rights on various occasions in the

context of the compelled production of documents or things by police and their powers of search and seizure.

17. In 1964, the majority in a Constitution Bench decision in *Shyam Lal Mohanlal v. State Of Gujarat* [1965 2 SCR 457] while considering Section 94(1), Code of Criminal Procedure, 1898 identical to Section 91(1), Cr.P.C. 1973] held that a notice under that provision to an 'accused person' amounts to compelling such person to be a witness against himself, thus violating Article 20(3) of the Constitution. Subsequently, in 1980, a Two Justices' bench decided *V. S. Kuttan Pillai v. Ramakrishnan & Anr.*, [(1980) 1 SCC 264] and held that search warrants could not be issued under Section 93(1)(a), Cr.P.C. *qua* an accused person compelling her to produce material that may otherwise be sought *via* notices issued under Section 91(1), Cr.P.C., for the reason that it compelled active participation on part of the accused, contrary to the guarantee against self-incrimination, under Article 20(3) of the Constitution.
18. Thus, due to interventions by this Hon'ble Court, the regime governing production of documents or things now prohibits the state from compelling accused persons to cooperate in an investigation against them. This has meant a complete prohibition in respect of any notice requiring such production to be issued to persons accused of an offence in accordance with the terms of Article 20(3) of the Constitution, and restrictions on the kind of cooperation that can be sought during search and seizure operations as well. However, there has yet been no engagement either by the statute or by this Hon'ble Court into the impact on the fundamental right to privacy of the manner in which law enforcement agencies compel production of documents or things.

SPECIFIC ISSUES CONCERNING DIGITAL DEVICES AND PREVIOUS CONSIDERATION BY COURTS IN INDIA

19. It is submitted that the extant legal regime compelling production of materials as identified above unequivocally applies to the mere production of digital devices, as these are 'things' of which production can be sought and which can be seized pursuant to a search. However, the issues being highlighted in the present petition arise once an investigation / inquiry moves beyond the mere production of a device and travels into the scrutiny of its contents. The effects of an unclear legal regime governing the seizures of digital devices *and the information found on them* are of a qualitatively different nature as compared to the physical realm. The information stored on personal digital devices is deeply intimate and inconceivably more revealing about an individual's life than anything held at a physical 'place', connected as they are to the cloud for housing data in most instances; furthermore, it is immensely mutable and movable, and vastly more susceptible to tampering than any material existing in the physical realm.

Some of the legal issues thus include:

- (i) Whether the extant legal regime, which is limited to the search of 'places' and the production of 'documents', can apply to *information* held on digital devices in its digital form?
- (ii) Assuming the present legal regime is applicable to digital devices, then the following issues arise:
 1. Determining the breadth of notices to compel production of any information held on devices: can law enforcement agencies demand turning over passcodes and complete access to digital devices, or must notices be sufficiently tailored in terms of the

- right to privacy and the law require justifications from officers for demanding access to the personal information of persons?
2. Determining whether any searches of seized digital devices, can be permitted without prior judicial scrutiny through a warrant? If so, under what circumstances would such warrantless searches for specific information be permitted?
 3. Determining whether general warrants under Section 93(1)(c), Cr.P.C. are permissible in respect of searching contents of digital devices?
 4. Determining the extent of cooperation that can be sought from a person during search of a digital device — would different standards apply to ‘accused’ persons and others?
- (iii) How ought the personal information that is accessed for purposes of investigations or inquiries be processed and stored to ensure respect for the right to privacy?
 - (iv) How ought the retention of personal information accessed by law enforcement agencies for purposes of investigations or inquiries be regulated, including the recognition of a mandatory deletion processes to ensure respect for the right to privacy?
 - (v) How ought accountability be ensured in case of data breaches of personal information that is accessed and retained by law enforcement agencies for purposes of investigations or inquiries?
20. As was unequivocally held by a Constitution Bench of this Hon’ble Court in *Justice (Retd.) K.S. Puttaswamy* [(2017) 10 SCC 1], it is imperative that the legal understanding of fundamental rights is not confined to a sense of the world as it existed in 1950. Rather, legal understanding of fundamental rights must be capable of adapting and evolving to the

changing socio-political and technological realities of the times, for them to sufficiently safeguard the individual dignity and autonomy of persons.

21. Indeed, in his famous - and subsequently vindicated - opinion in *Olmstead vs United States* [277 U.S. 438 (1928)], Justice Brandeis articulated this wisdom for the ages, when he noted that:

“When the Fourth and Fifth Amendments were adopted, “the form that evil had theretofore taken” had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify — a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life — a seizure effected, if need be, by breaking and entry. Protection against such invasion of “the sanctities of a man’s home and the privacies of life” was provided in the Fourth and Fifth Amendments by specific language. But “time works changes, brings into existence new conditions and purposes.” Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.”

22. It is respectfully submitted that the extremely limited occasions on which issues pertaining to search and seizure of digital devices have arisen for consideration before Hon’ble High Courts, this evolutionary and contextual approach has been found lacking. For instance, by an

extremely narrow reading of this Hon'ble Court's decisions in *State of Bombay v. Kathi Kalu Oghad* [(1962) 3 SCR 10] and *Smt. Selvi v. State of Karnataka* [(2010) 7 SCC 263], the Hon'ble Karnataka High Court in *Virendra Khanna v. State of Karnataka & Ors.* [(2021) 3 AIR Kant R 455] has held that an accused person, in custody, and from whom digital devices are recovered, can be compelled to give information to unlock such devices. It has further held that law enforcement agencies are competent to demand untrammelled access to the information on such devices by exercising the powers under Chapter VIII, Cr.P.C. (while also passing certain guidelines for securing the chain of custody and integrity of seized material). In a manner *ex facie* contrary to the decision in *Justice (Retd.) K.S. Puttaswamy* [(2017) 10 SCC 1], the Hon'ble High Court simply declared one's privacy as being subservient to law enforcement interests of crime control without entering any proportionality analysis whatsoever.

23. The consequences of such a view have implicitly served to authorise police and other law enforcement agencies to demand access from *any* person of their digital devices, while carrying out general searches of entire districts — popularly termed as 'cordon searches'. In a manner entirely unknown to law and in the teeth of the tests of proportionality, police officers demand access to *inter alia* personal mobile phones for random searches of their contents, purportedly for securing state interests such as preventing crimes, and not for purposes of any investigation or inquiry. Almost every such instance results in acquiescence by the persons out of fear, resulting in an unconstitutional waiver of their fundamental rights in the face of an *ex facie* illegal action by state authorities. A true copy of article titled 'Hyderabad cops are stopping people on the road, checking WhatsApp chats for 'drugs'' is annexed

herewith as ANNEXURE P-4(130-132). A true copy of an article titled 'Are Bengaluru cops 'forcing' locals to hand over phones to check WhatsApp, photos?' is annexed herewith as ANNEXURE P-5(133-135). A true copy of an article titled 'Gujarat: Digital combing in Gujarat to curb porn circulation' is annexed herewith as ANNEXURE P-6(136-137)

24. Besides oppressive state power being witnessed in the context of gaining access to devices, there have been multiple instances where personal data or information such as communication between persons accessed by law enforcement agencies during a probe by way of searching the contents of a digital device, finds its way into the hands of media and becomes the basis for media-trials, reflecting the absence of proper measures to ensure safety of data that is being accessed purportedly in the pursuit of investigations.
25. Specifically, the Petitioner states that the prevailing absence of clarity on the legal position and *prima facie* support by subordinate Courts of legal standards in derogation of proportionality and the right to privacy, have resulted in an implicit legal sanction for state authorities demanding journalists to provide complete access to the information held on their digital devices, and initiating seizures of these devices and all the information stored on them, often without any apparent nexus to any ongoing inquiry or investigation.
26. A consequence of such a state of affairs has been to cast serious impediments on the exercise of the basic right to practice one's profession, as journalists are constantly in fear of having to disclose confidential sources and lose access to their work which may be stored digitally, where such work often pertains to newsworthy political events

concerning elected representatives and / or government officials. The inability to secure confidentiality of sources does not only strike a telling blow on a journalist's ability to practice her profession, but also casts a chilling effect across society especially on those willing to repose their faith and trust in such journalists despite obvious fear for their life and safety [see, *Shreya Singhal v. Union of India*, (2015) 6 SCC 1].

27. Therefore, the illustrative list of issues and the limited engagement with them thus far, along with the serious and debilitating impact of the *status quo* on rights of persons especially those from the journalist community, reflects an urgent and pressing requirement for intervention by this Hon'ble Court to, *inter alia*, ensure a respect for the right to privacy in the realm of how state agencies handle digital devices in the context of inquiries and investigations. The issues, primarily, require an interpretation of statutory provisions on their own terms and *vis-à-vis* various fundamental rights guaranteed under the Constitution, which is well-within the jurisdiction of this Hon'ble Court as the custodian of the Constitution and rule of law.
28. Further, in respect of consequential directions to agencies to secure compliance with the interpretive findings of this Hon'ble Court, it is submitted that such directions are also well-within the jurisdiction of this Hon'ble Court. On multiple previous occasions, this Hon'ble Court has issued directives regulating different facets of how state actors exercise coercive powers afforded to them under law to ensure respect for the fundamental rights of persons guaranteed under the Constitution of India. Reference in this regard may be had to *D.K. Basu v. State of West Bengal & Ors.* [(1997) 1 SCC 416], *Arnesh Kumar v. State Of Bihar* [(2014) 8 SCC 273], *Anuradha Bhasin v. Union of India & Ors.* [(2020) 3 SCC

637], and *Paramvir Singh Saini v. Baljit Singh & Ors.* [(2021) 1 SCC 184].

29. Besides police, the directions from this Hon'ble Court have also extended to courts, by *inter alia* establishing legal frameworks to safeguard not only investigative interests but also ensure respect for fundamental rights. In *Smt. Selvi v. State of Karnataka (supra)*, this Hon'ble Court while holding certain forensic tests as implicating the rights under Articles 20(3) and 21 of the Constitution, further provided a legal framework for enabling police to resort to such tests in the future — by mandating prior informed consent with judicial oversight. In *Ritesh Sinha v. State of U.P.* [(2019) 8 SCC 1] this Hon'ble Court noticed the absence of any legal framework governing taking of voice exemplars for purposes of criminal investigations and exercised its inherent powers under Article 142 of the Constitution to provide this legal basis to secure interests of the law enforcement agencies while ensuring respect for the fundamental rights of persons. More recently, in *Satyender Kumar Antil v. CBI* [2022 SCC OnLine SC 825, judgment dated July 11, 2022 in M.A. No. 1849 of 2021 in SLP (Crl.) No. 5191 of 2021] this Hon'ble Court issued guidelines to aid trial courts in exercising their jurisdiction to grant bail. Thus, the consequential reliefs prayed for are well within the jurisdiction of this Hon'ble Court.

CONSIDERATION OF COMPARATIVE APPROACHES

30. Issues regarding access to the contents of digital devices in the context of criminal investigations have arisen across jurisdictions globally over the recent decades, prompting several common law countries to either amend statutory provisions or to introduce entirely new statutes to provide sufficient legal basis for law enforcement agencies to secure access for

purposes of investigations or inquiries, in a manner that respects basic rights of privacy and against compelled self-incrimination.

Asia

31. Provisions similar to the Cr.P.C., 1973 can be found in Singapore and Malaysia, owing to their colonial connections with India. However, unlike India, both these jurisdictions have carried out amendments of their Codes of Criminal Procedure, to provide a sufficient legal basis for carrying out a search of the contents of digital devices.
32. Section 39 of the Singapore Criminal Procedure Code, 2010 specifically empowers the police to search the contents of a 'computer' (expansively defined) during the course of an inquiry or investigation where the said computer is either believed to have been used in connection with the offence being investigated, or holds evidence in respect of commission of such offence, and demand assistance from persons who have the capability to offer such assistance, including a requirement to provide authentication of accounts, etc. It is crucial to note that unlike India, Singapore does not recognise a fundamental right to privacy. A true copy of Section 39 of the Singapore Criminal Procedure Code, 2010 is annexed herewith as **ANNEXURE P-7(138-170)**.
33. Section 116B of the Malaysian Criminal Procedure Code, 2012 specifically empowers senior police officials carrying out a search to demand access to computerised data which may be stored on a computer, where access has been explained to include passwords etc. required to render the data comprehensible. Malaysian law, whilst having a data protection law, does not recognise a fundamental right to privacy. A true

copy of Section 116B of the Malaysian Criminal Procedure Code, 2012 is annexed herewith as ANNEXURE P-8(171-196)

34. Like India, Hong Kong recognises a basic right to privacy under Article 30 of the Basic Hong Kong Law (BL 30) and Article 14(1) of the Hong Kong Bill of Rights (BOR14), except in cases where inspection is allowed in accordance with legal procedures for public safety or investigation into crime. BOR14 specifically protects privacy beyond communications. Sections 50(6) and (7) of the Hong Kong Police Force Ordinance do not make specific reference to digital devices but provide for search of a place or a document in relation to a suspected person.
35. In *Sham Wing Kan v. Commissioner of Police* [(2020) 2 HKLRD 529] the Hong Kong Court of Appeal, while considering how search and seizure of mobile and similar devices from accused persons incident to arrest can be conducted in a manner that is compatible with BL30 and BOR 14, made various observations regarding the heightened privacy interests involved in accessing personal digital devices. In light of this, it held that ordinarily warrants must always be obtained for such searches, limiting warrantless searches to be permitted only in exceptional circumstances. A true copy of BL30 and BOR 14 is annexed herewith as ANNEXURE P-9(197-211).

Canada

36. In Canada, cell-phones users are generally held to have a reasonable expectation of privacy, determination of which varies from case-to-case. Courts have found that there is a reasonable expectation of privacy by cell phone users with respect to their phone, and pertinently, the text messages contained therein, as well the messages contained in the

receiver's phone and the service providers' records. [See *R v. Polius* (2009) 196 CRR (2d) 288 (Ont. SCJ) at para 50, *R v. O. (T.)* 2010 ONCJ 334 at para 42, 46, *R v. Artis*, 2016 ONSC 2050 at para 12, *R v. Marakah*, 2017 SCC 59 at para 59, and *R v. Jones* 2017 SCC 60 at para 55]

37. In *R. v. Fearon* [2014 SCC 77, at Para 56] the Supreme Court of Canada found that there was a lower expectation of privacy when cell phones were searched incidental to a lawful arrest. Accordingly, the Court held that police officers will be justified in searching a cell phone or similar device incidental to arrest only when: “(1) *The arrest was lawful; (2) The search is truly incidental to the arrest in that the police have a reason based on a valid law enforcement purpose to conduct the search, and that reason is objectively reasonable. The valid law enforcement purposes in this context are: (a) Protecting the police, the accused, or the public; (b) Preserving evidence; or (c) Discovering evidence, including locating additional suspects, in situations in which the investigation will be stymied or significantly hampered absent the ability to promptly search the cell phone incident to arrest; (3) The nature and the extent of the search are tailored to the purpose of the search; and (4) The police take detailed notes of what they have examined on the device and how it was searched.*” (Para 83).
38. Furthermore, courts in Canadian provinces have also considered the issue of whether a person can be compelled to unlock a digital device, either by way of providing a passcode or by providing a biometric impression. In *R v. Shergill* [2019 ONCJ 54 (CanLII)] it was held by the Ontario Court of Justice that compelling an individual to furnish such information would implicate the privilege against self-incrimination.

United Kingdom

39. In the United Kingdom, the Police and Criminal Evidence Act, 1984 grants wide powers of search and seizure to the Police. Section 17 and 18 therein permit entry and search without a warrant only for the purposes of arrest (in certain offences) or after arrest. Section 32 permits a warrantless search upon arrest in certain circumstances. In all other cases, procurement of a search warrant is mandatory. It is important to note that neither Part I (Powers to Stop and Search), nor Part II (Powers of Entry, Search and Seizure), nor Part III (Arrest) of the Police and Criminal Evidence Act, 1984 specifically provide for search of electronic devices.
40. Section 49 of Regulation of Investigatory Powers Act, 2000 grants power to the police and other public authorities to compel disclosure of any key or password that may be restricting access to ‘protected information’ that is relevant for *inter alia* purposes of an investigation. The key disclosure requirement is tempered with numerous safeguards, such as proportionality assessments to determine if no other alternative is available, and statutory requirements to issue a formal notice describing the protected information to which access is sought, and limits access only to such information thereafter. A true copy of Part III the Regulation of Investigatory Powers Act, 2000 containing Section 49 is annexed herewith as ANNEXURE P-10(212-238).
41. In *Privacy International v. Investigatory Powers Tribunal* [(2021) EWHC 27 (Admin)], the High Court (Queen's Bench Division) considered whether Section 5 of the Intelligence Services Act, 1994 (which provides for general warrants) permitted issuance of a ‘thematic’ computer hacking warrant “authorising acts in respect of an entire class of people or an entire class of such acts.” The High Court reaffirmed the

aversion of common law to general warrants (paragraphs 39 to 51) and held that a warrant issued under the said provision was lawful if it was “*sufficiently specific for the property concerned to be objectively ascertainable on the face of the warrant.*” A true copy of Section 5 of the Intelligence Services Act, 1994 is annexed herewith as ANNEXURE P-11(239-244).

Australia

42. In the Commonwealth, Queensland, South Australia, and Victoria, laws have been introduced to empower magistrates to order individuals to provide the police with access to devices in the context of investigations.
43. In South Australia, Part 16A of the Summary Offences Act, 1953 (SA), particularly Section 74BR allows a magistrate to require certain specified persons to provide any information or assistance that is reasonable or necessary to allow a police officer to access, examine, or perform any function in relation to, any data held on any computer or data storage device (refusal to order is punishable upto 5 years). This provision, however, is applicable only when there are reasonable grounds to suspect that data held may afford evidence of a child exploitation offence. A true copy of Section 74BR of the Summary Offences Act, 1953 (SA) is annexed herewith as ANNEXURE P-12(245-253).
44. In the Commonwealth, Section 3LA of the Crimes Act 1914 (Cth) allows magistrates to pass orders directing specified persons to provide any information or assistance reasonable and necessary to allow the police to access data held in, or accessible from, a computer or data storage device. A true copy of Section 3LA of the Crimes Act 1914 (Cth) is annexed herewith as ANNEXURE P-13(254-281).

45. In Queensland, Sections 154, 154A and 154B of the Police Powers and Responsibilities Act, 2000 (Qld) empower the magistrate to order, while issuing a search warrant, or even thereafter, a specified person to give a police officer access to the storage device and the access information and any other information or assistance necessary for the police officer to be able to use the storage device to gain access to stored information that is accessible only by using the access information. A true copy of Sections 154, 154A and 154B of the Police Powers and Responsibilities Act, 2000 (Qld) is annexed herewith as ANNEXURE P-14(282-329).
46. In Victoria, Section 465AAA of the Crimes Act, 1958 empowers a magistrate issuing a search warrant under Section 465 therein to authorise a police officer to direct a specified person to provide any information or assistance that is reasonable and necessary to allow the police officer to access data held in, or accessible from, a computer or data storage. A true copy of Section 465AAA of the Crimes Act, 1958 in Victoria is annexed herewith as ANNEXURE P-15(330-357.)

European Union

47. In Europe, Human Rights are guaranteed by the European Convention on Human Rights, 1950 [Convention]. Article 8 of the Convention guarantees the right to respect for one's private and family life, his home and his correspondence. This right may be interfered with only if it is a) in accordance with law; b) necessary in a democratic society; and c) in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of

others. A true copy of Article 8 of the European Convention on Human Rights, 1950 is annexed herewith as ANNEXURE P-16(358-360).

48. Most countries in the European Union are parties to the Convention on Cybercrime, 2001 which is also known as the Budapest Convention on Cybercrime [**'Budapest Convention'**]. Article 18(1) of the Budapest Convention is similar to Section 91, Cr.P.C. but with additional safeguards. It asks signatory states to adopt legislative measures to empower competent authorities to order a person in its territory to submit 'specified computer data' in a person's possession or control, which is stored in a computer system or a computer-data storage medium. Article 18(2) states the powers conferred by Article 18(1) shall be subject to Article 15 which in turn requires laws to incorporate principles of proportionality to adequately protect human rights including rights guaranteed under the Convention, such as Article 8, the 1966 International Covenant on Civil and Political Rights, and other applicable international human rights instruments.
49. Article 19(1) of the Budapest Convention delimits the circumstances in which signatory countries may search or access computer resources. It requires signatory countries to adopt 'such legislative and other measures' as may be necessary to empower its competent authorities to search or access a 'computer system or part of it and computer data stored therein'. Article 19(3) requires these legislative and other measures to include the power to seize a computer system, make and retain copies of computer data, maintain the integrity of the relevant stored computer data and remove computer data. Article 19(5) states that powers conferred by Article 19(1) shall be subject to Article 15 which, as stated above, requires laws to incorporate principles of proportionality and provide for

adequate protection of human rights including those arising pursuant to the stated international human rights treaties. A true copy of Articles 18 and 19 of the Budapest Convention on Cybercrime is annexed herewith as ANNEXURE P-17(**361-363**).

50. Several signatory states of the European Union have implemented the Budapest Convention. For example, in 2008, Italy amended its Code of Criminal Procedure, 1988 [CCP]. Article 247 of CCP specifically provides how computer-systems may be searched or seized, and it requires that searches should be conducted only if there are reasonable grounds to believe that the computer-system in question was used to commit an offence or is related to an offence. Similarly, Portugal (Law 109/2009), Spain (Ley Organica 13/2015), Romania (Law 161/2001) and France (The Law on the Confidence in the Digital Economy of 2004), enacted laws or amended existing laws to incorporate the Budapest Convention in their domestic laws. A true copy of Article 247 of the Italian Code of Criminal Procedure, 1988 is annexed herewith as ANNEXURE P-18(**364**).

Judicial Engagement in the European Union

51. In *Ivashchenko v. Russia*, Application No. 61064/10 (Decided February 13, 2018), the applicant was a photographer returning to Russia on foot after travelling to Abkhazia. At the border, customs authorities examined the applicant and copied personal and professional data found on his laptop. Subsequently, this data was analysed by a specialist and retained for over two years. The applicant questioned the authorities' power to copy data. The respondent-state defended the action by relying on the Customs Code of the Russian Federation of 28 May 2003 ['Customs Code'], which permitted inspection of goods transferred across borders.

The respondent-state contended that Article 11 of the Customs Code defined 'goods' as moveable or immovable property, thus the laptop fell within the definition of 'goods' and could be inspected. The European Court of Human Rights rejected this contention and held that the Customs Code did not provide a legal basis for copying electronic data contained in a 'container' such as a laptop (para 80). As such, actions of the customs authorities violated Article 8 of the Convention. A true copy of Article 11 of the Customs Code of the Russian Federation of 28 May 2003 is annexed herewith as ANNEXURE P-19.(365-368)

52. In the case of *Trabajo Rueda v. Spain*, Application No. 32600/12 (Decided on May 30, 2017), the European Court of Human Rights held that the seizure of the applicant's personal computer was contrary to Article 8. Police seized the applicant's personal computer on the ground that it contained pornographic material but did not obtain prior judicial authorisation. The Court observed that a prior judicial authorisation was required when an individual's private life was likely to be infringed, except in emergency situations, in which case subsequent judicial scrutiny was possible. In the applicant's case, prior judicial authorisation was not obtained even though it could have been obtained without impeding the investigation.
53. In *Beghal v. United Kingdom*, Application No. 4755/2016 (Decided on February 28, 2019), the European Court of Human Rights considered an application challenging the decision of police to stop, examine and search the applicant in the exercise of powers under Schedule 7 of the Terrorism Act, 2000. Schedule 7 *inter alia* permitted police to search persons to determine if they have been involved in the commission, instigation or preparation of acts of terrorism. The European Court of Human Rights

held that Schedule 7 powers were not 'in accordance with law' and violated Article 8 of the Convention, as Schedule 7 *inter alia* permitted search even in the absence of 'reasonable suspicion' (Para 109). Moreover, it did not contain adequate legal safeguards to prevent abuse. A true copy of Schedule 7 of the Terrorism Act, 2000 of the United Kingdom is annexed herewith as ANNEXURE P-20. (369-408)

54. In *Sargava v. Estonia*, Application No. 689/19 (Decided on November 16, 2021), the applicant, a lawyer, approached the European Court of Human Rights, questioning seizure and examination of his laptop and mobile phone by law enforcement. The applicant contended that his devices were seized and examined in a manner which did not sufficiently protect privileged communication between him and his clients. The Court held that Estonian domestic law did not contain any procedure or safeguards to protect legal professional privilege in such search actions (para 103), which meant that domestic law fell short of the requirement that interference must be in accordance with law as per Article 8 of the Convention (para 109).
55. In *Funke v France*, Application No. 10828/84 (Decided on February 25, 1993), the applicant was convicted for refusing to produce his bank statements to the Customs Authority after admitting that he had bank accounts abroad. The applicant contended his conviction violated his right against self-incrimination, and the European Court of Human Rights agreed with this contention and held that the authorities decision to compel the applicant to contribute to incriminating himself violated the right to fair trial guaranteed by the Article 6 of the Convention.

United States of America

56. The Fourth Amendment of the US Constitution was codified in response to the usage of general warrants and writs of assistance in the colonial era, and entrenched the basic common law principle - set out in *Entick vs Carrington* [1765] EWHC KB J98 - against general warrants. The Fourth Amendment protects people from unreasonable search and seizures. It requires warrants to be issued upon 'probable cause', describing the place to be searched, and the persons or things to be seized. Few exceptions like good faith, plain view doctrine, exigent circumstances, consent, administrative searches, search of automobiles, and frisking have been identified narrowly through case law, and warrantless search may be allowed only in such circumstances.
57. In *Riley v. California* [573 U.S. 373 (2014)], the Supreme Court of the United States ruled that the same standards for search as applicable to physical items could not be applied to search of mobile phones. It ruled that warrantless search of a mobile phone incidental to arrest violated the Fourth Amendment. The Court found that the seizure of physical items differed both qualitatively and quantitatively with seizure of mobile phones which contain a wealth of highly sensitive data, search of which raises privacy concerns. The Court highlighted various factors, such as high storage capacities of cell phones, the nature of information stored in them, external data connected through cloud computing etc. to hold that mobile phones were a "*pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.*"
58. The Fifth Amendment to the US Constitution protects persons from self-incrimination and double jeopardy, and also mandates that no persons can be deprived of life, liberty, or property, without due process of law. In

Katelin Eunjoo Seo v. State of Indiana [Supreme Court Case No. 18S-CR-595, decided on June 23, 2020], the Indiana Supreme Court found that securing a warrant to force Seo (the Appellant in the case) to unlock her iPhone would violate her Fifth Amendment right against self-incrimination. The Court found that Seo would be providing law enforcement with information they did not have by the act of unlocking the phone. Such information can then be used against her for prosecution, which was prohibited by the Fifth Amendment protection.

59. *In the Matter of the Search of a Residence in Oakland, California* [354 F. Supp. 3d 1010 (N.D. Cal. 2019)] the United States Magistrate Judge of the United States District Court, Northern District of California, denied a search warrant application which sought to compel or otherwise utilise fingers, thumbs, facial recognition, optical/iris, or any other biometric feature of individuals (in the context of investigation) to unlock electronic devices. The Court ruled that use of biometrics to unlock devices was analogous to use of passwords, and compulsion to use biometrics information violated the Fourth and Fifth Amendment rights. The motion for review against this judgment was dismissed as moot.

Summation of International Practices

60. It is respectfully submitted that three clear trends emerge from a scrutiny of international jurisprudence on the issue of accessing the contents of personal digital devices.
61. *First*, almost all jurisdictions demonstrate the need to have a clear legal basis to authorise law enforcement agencies in accessing such personal information, with statutes clearly demarcating the scope and extent of such powers to ensure respect for privacy.

62. *Second*, almost all jurisdictions today impose the need for law enforcement agencies to obtain a prior judicial warrant for gaining access to the contents of a digital device — even where a separate issue may arise as to whether cooperating with the warrant by giving access to the device implicates the right against compelled self-incrimination. Search of a digital device without warrant has been rendered exceptional, usually only limited to arrests.
63. *Third*, and finally, there is unanimous recognition in jurisdictions abroad that untrammelled and unbridled access to personal digital devices in pursuit of purported state interests is illegal and casts a disproportionate impact on the right to privacy.
64. In light of the above facts and circumstances, and aggrieved by the lack of a clear legal basis governing the access of the contents of digital devices by law enforcement agencies in a manner consistent with fundamental rights, the Petitioner prefers the present petition on the following, amongst other, grounds.

GROUND

- A. BECAUSE the search and seizure of digital devices carries serious rights' implications for all persons, directly impacting the fundamental right to privacy, which is inherent in Articles 14, 19 and 21 of the Constitution. Further, such law enforcement actions when carried out against persons arrested / accused of offences also triggers the fundamental right against self-incrimination guaranteed under Article 20(3) of the Constitution of India.

- B. BECAUSE the use of personal digital devices is today all-pervasive and a necessary component of individuals seeking the fullest expression of their basic freedoms and exercising their right to life with dignity. Specifically, personal digital devices are integral to the journalistic profession, built as it is on communication, networks, and secure storage of confidential sources and information. Journalists are necessarily reliant on such devices today to be able to freely and effectively exercise their profession. They not only store information in the nature of unpublished work product, but also information which may have a critical impact on the security of other persons such as confidential informants and sources of information.
- C. BECAUSE the implication of privacy interests is significantly higher in the context of personal digital devices as compared to other personal effects, not only on account of the significant amounts of data that these devices contain about one's intimate personal life, but furthermore because it is increasingly common for such devices to be linked via internet services to remote repositories of data in the "cloud". Thereby, digital devices serve as a gateway to additional information that may not be held on the device itself. Ultimately all this information (on the device and on the cloud) is extremely vulnerable, being so easily transmissible and portable, thereby warranting higher protection under the rule of law.
- D. BECAUSE the extant legal regime governing seizures and searches in India is *ex facie* inapplicable to searches of the contents of digital devices and thereby renders any such action by law enforcement agencies illegal for want of a statutory legal basis. Thus, these infractions of fundamental rights carried out today are *ex facie* unconstitutional.

E. BECAUSE there is an uncontested and unequivocal recognition across the globe of the rights' implications at stake in searches or seizures of digital devices being unique and incomparable to searches or seizures for material in the physical realm, requiring special statutory provisions and legal rules for governing the former.

Arrested / Accused persons and the Right against Compelled Self-Incrimination

F. BECAUSE Article 20(3) of the Constitution guarantees to all persons accused of an offence a fundamental right against being compelled to be a witness against themselves. All persons arrested by the police and subject to personal searches would be squarely covered by the phrase 'accused' of an offence and thereby triggering the right under Article 20(3).

G. BECAUSE demanding cooperation of arrested persons by providing access to seized personal devices, by way of furnishing decryption keys / passcodes / biometric IDs etc., is *ex facie* compelling in nature for it coerces an accused person to cooperate in the investigation against him. The scenario is *in pari materia* with an accused person being furnished with a notice to produce information under Section 91, Cr.P.C. or being served with a warrant for such information under Section 93(1)(a), Cr.P.C.

H. BECAUSE the phrase 'to be a witness' against oneself found in Article 20(3) has been consistently explained by this Hon'ble Court as not merely being limited to furnishing evidence at trial but extending to the pre-trial stage of the process and extending to furnishing any information (including documentary evidence) that can furnish a link in the chain of evidence.

- I. BECAUSE this Hon'ble Court has held that the only exception to the rule pertains to material that is not relevant to the chain of evidence *per se* and is only useful to the investigation on account of it being used for purposes of comparison with material gathered by the investigating agencies of their own accord. Thus, compelled seizure of fingerprints, blood samples, voice exemplars, handwriting samples, etc. is permissible on account of such material not being capable of furnishing a link in the chain of evidence, as it is only relevant for purposes of comparison with material obtained by the police during investigation. Compelling persons to provide decryption keys / passcodes / biometric IDs etc. enabling access to personal digital devices seized from them does not furnish material for a comparison purpose, but is a fact intrinsically relevant and capable of furnishing a link in the chain of evidence by itself.
- J. BECAUSE this Hon'ble Court in *Selvi v. State of Karnataka (2010) 7 SCC 263* has expressly held that the right against compelled self-incrimination cannot be made contingent on law enforcement agency's determination of whether or not the information is 'incriminatory' or 'exculpatory' as it would render the right nugatory.
- K. BECAUSE providing access to personal digital devices furnishes a clear link in the chain of evidence and therefore completes the requirements for Article 20(3). The mere fact of providing access confirms that the accused person has control over the device in question, and enables a presumption that the accused is responsible for and aware of the contents of the device.

- L. BECAUSE the fact of providing access to personal digital devices cannot be separated from the contents of the device. A digital device in the nature of a personal phone or a computer contains intimate information created in the past like a diary that can be seen as a snapshot of life being separate from one's consciousness. Additionally, it is an active companion for essential daily tasks, in which information is continuously and contemporaneously generated, as a result of conscious actions made by the person — conversations started, subscriptions availed, meetings scheduled, reminders set, etc. Such devices are an extension of the self and offer a continuous and contemporary insight into one's life.
- M. BECAUSE there are adequate technological solutions available with a state agency to obtain access into the digital device without any assistance being rendered by a person; consequently, on grounds of proportionality, there is no justification for the State e to demand that the accused person must cooperate in her prosecution by providing access to her digital devices and thereby invite the state agency to scrutinise the most private recesses of her life.

Unique Privacy Interests for Arrested / Accused Persons

- N. BECAUSE this Hon'ble Court has recognised that the fundamental right against compelled self-incrimination does not operate in a silo but coexists with the right to life and personal liberty guaranteed under Article 21, and the fundamental right to privacy (including the right to mental privacy), which is inherent to Article 21.
- O. BECAUSE the wealth of information contained on personal digital devices, including information that is created in the past but also information that is contemporaneously and continuously being generated

on the device, creates obvious implications for the right to privacy of persons controlling the said device where law enforcement agencies seek access to such information.

- P. BECAUSE the extant legal regime governing production of material and searches and seizures — though *ex facie* inapplicable to digital devices — nevertheless reflects a clear requirement for law enforcement agencies to demonstrate an investigative purpose behind such privacy-intruding actions and does not permit a pure roving and fishing inquiry allowing *post facto* justifications to be furnished. Furthermore, the powers for carrying out any searches without warrant does not empower police to carry out general searches of the kind sanctioned by warrants under Section 93(1)(c), Cr.P.C.
- Q. BECAUSE, therefore, enabling law enforcement agencies to have unbridled and untrammelled access to personal digital devices merely on the strength of an untested, unverified allegation against an individual is not only grossly disproportionate to the any perceived state interests in pursuit of the case but also *ipso facto* transforms the investigation into a specific offence on the basis of some information independent of the individual, into a roving and fishing inquiry based on nothing other than material that the individual herself is compelled to furnish to the authorities and destroys the right to privacy.
- R. BECAUSE a bald assertion that criminal activity deserves no privacy does not offer any justification to the disproportionate intrusion into the most intimate details of the personal lives of individuals and is placing the cart before the horse — it denudes the presumption of innocence of

all meaning by presuming that a single accusation ought to deprive an individual of any privacy over the various facets of her life.

Right to Privacy

- S. BECAUSE the right to privacy is inherent to the very concept of individual dignity sought to be protected by the Constitution, and finds expression in personal digital devices of individuals today, which have been recognised as being nothing short of a part of the human anatomy itself.
- T. BECAUSE a Constitution Bench of this Hon'ble Court in *Justice (Retd.) K.S. Puttaswamy* unanimously declared the observations in *M.P. Sharma & Ors. v. Satish Chandra & Ors.* [1954 SCR 1077] as being *per incuriam* and therefore it is natural that any regime of search and seizure must operate in a manner consistent with the fundamental right to privacy.
- U. BECAUSE the exercise of search and seizure powers, or powers to compel the production of documents or things, by law enforcement agencies to get access to the contents to these devices necessarily implicates this essential privacy interest of individuals inherent in Articles 14, 19 and 21 of the Constitution. Persons who rely upon digital devices as opposed to those who do not form a separate class which is disproportionately and unequally at risk of intrusive state action. Such persons in turn rely upon their digital devices to exercise fundamental freedoms and, further, rely upon them to fully exercise their autonomy and express their intrinsic dignity.
- V. BECAUSE personal digital devices do not only contain sensitive personal data in the nature of private correspondence but also sensitive information

about one's health and well-being, sexual preferences, political beliefs and ideologies, as well as sensitive information about one's financial affairs, in respect of which all persons enjoy a reasonable expectation of privacy.

- W. BECAUSE the privacy interests of journalists are specifically at risk where intrusion of digital devices is concerned, as today these professionals are heavily reliant on such devices for every element of their trade — from use of the communicative aspect of these devices to interact with sources of information, including confidential informants, to using the processing and storage capacity of these devices to gather and store information which is being developed for publication.
- X. BECAUSE any state action implicating the right to privacy must satisfy the legal tests laid out under Articles 14, 19 and 21 of the Constitution, as have been explained by this Hon'ble Court, for such state action to be upheld as being a valid and constitutional infringement of a person's privacy.
- Y. BECAUSE this Hon'ble Court has adopted a four-fold analysis as suitable to determine the validity of state action infringing any of the fundamental rights, requiring the courts to determine (i) whether the impugned action has any legal basis, (ii) whether it is pursuing a necessary state interest, (iii) whether the state interest is proportionate to the harm to fundamental rights, and (iv) whether sufficient procedural safeguards exist to secure the fundamental rights.

Legal Basis

- Z. BECAUSE the requirement for a valid, statutory legal basis, supporting the rights-infringing state action is a pre-condition provided under Article 21 of the Constitution — there must be a procedure established by law for a state action to validity infringe the right to life and personal liberty of which the right to privacy is an intrinsic component.
- AA. BECAUSE there is no valid legal basis for enabling state agencies to either compel production of the contents of a digital device or to subject them to a search or seizure operation. No legal provisions provide for state agencies to gain access to a locked device, search it, process its contents and / or delete any copies made in the process.
- BB. BECAUSE extant legal provisions under the Cr.P.C. or special acts confine themselves to requiring production of ‘documents’ or ‘things’, or to enable law enforcement agencies to conduct searches of ‘places’ to seize any such items. A bare perusal of the statutes confirms that none of the relevant provisions pertains to ‘electronic records’, and therefore do not enable the law enforcement agencies to seek production of such items. Further, digital devices are not ‘places’ thereby excluding application of search provisions as well.
- CC. BECAUSE recognising this limitation of provisions originally crafted in the colonial codes, other jurisdictions which were formerly colonies of the British have taken steps to modify their statutory provisions to provide the necessary legal basis for law enforcement agencies to compel production of the contents of digital devices or to search their contents for themselves.

DD. BECAUSE absence of a valid legal basis provided in statutes renders the impugned state action infringing fundamental rights entirely incapable of justification and *ex facie* unconstitutional.

Necessity

EE. BECAUSE assuming there exists a valid legal basis for the impugned state action—the compelled production of contents of digital devices or their search and seizure—it must nevertheless be supported by a necessary state objective to justify intrusion of any fundamental rights.

FF. BECAUSE the purported necessity behind empowering state agencies to examine the contents of digital devices is the legitimate state interest in empowering police to investigate commission of crimes; to ensure that the state agencies have sufficient investigatory powers to collect evidence in the aid of prosecution of crime.

GG. BECAUSE the legitimate state interest in ensuring adequate powers for pursuit of criminal investigations entails enabling police to pursue the truth behind allegations regarding commission of offences which have occurred in the past, where the source behind the allegations is not the target of the investigation itself.

HH. BECAUSE it is well-settled that the legal process governing criminal investigation and prosecution of offences is punitive and not preventive. A broader view of the state interest at stake would necessarily imply allowing state agencies to demand untrammelled access to one's private life in aid of the nebulous notion of 'crime-prevention', which would result in a entirely demolishing the very essence of Article 21 and enlarge the limited realm of preventive powers beyond recognition.

- II. BECAUSE the pursuit of an investigation into commission of alleged offences as per law does not permit the state agencies to engage in a roving and fishing inquiry by rendering individual autonomy and dignity entirely subject to the state upon the mere foisting of accusations against a person. Allowing roving and fishing inquiries is beyond any necessary or legitimate state interest in the investigation and prosecution of crime.
- JJ. BECAUSE permitting a roving and fishing inquiry by enabling state agencies to demand access to the most intimate recesses of one's personal life handily contained in their personal digital devices contemplates a complete surrender of individual dignity of all or any persons to the might of the state upon the mere existence of any allegations regarding commission of offences and thus results in perverting the foundations of the rule of law.
- KK. BECAUSE providing untrammelled access to personal digital devices by way of warrantless searches or general searches authorised by warrants results in providing state agencies a ringside view into the most intimate details of one's life which may well be entirely unconnected and unnecessary in the pursuit of any alleged offence. Consequently, such a regime casts a wide shadow upon all persons leaving them fearful of such easy intrusions into their privacy, resulting in a chilling effect notably curtailing the fullest expression of individual dignity and the fundamental freedoms guaranteed by the Constitution.

Proportionality

- LL. BECAUSE this Hon'ble Court has clarified that a proportionality analysis of any impugned state action restricting rights requires determining (i) the

existence of a legitimate goal, (ii) its suitability for achieving this goal, (iii) it being the least restrictive alternative available, and (iv) it not having a disproportionate impact on the rights-holder. Providing untrammelled and unrestricted access to personal digital devices of persons and infringing their right to privacy as a result, purportedly in pursuit of investigations, does not withstand such an analysis.

- MM. BECAUSE the perceived legitimate state interest in pursuing investigations into alleged offences is intrinsically linked to a specific offence and does not entail sanctioning a roving and fishing inquiry by providing state agencies a ringside view into one's personal life, which is the natural and obvious consequence of allowing state agencies unbridled access to the contents of personal digital devices.
- NN. BECAUSE the requirement of proportionality extends to each and every component of the transaction — from the manner of gaining access to the contents of digital devices, to searching them and making copies of the data for analysis or processing. At each stage, it is imperative for the state action to be limited to no more than necessary intrusions into the sacred space of private thought and action.
- OO. BECAUSE the requirement of proportionality demands that state agencies be provided access to no more than whatever is the information necessary for pursuing investigative interests, which in turn requires state agencies to clearly demarcate the relevant investigative interests which may be served by intruding the privacy of a person and demanding access to the contents of her personal digital devices.

○

46

- PP. BECAUSE the only manner to adequately ensure that state agencies are accountable and do not proceed to disproportionately infringe the privacy of persons is to require prior judicial intervention as a norm, enabling the law enforcement agency to proceed without warrant only where they can demonstrate a real and active danger of any destruction of evidence being occasioned in the time it takes to secure a warrant.
- QQ. BECAUSE the requirement of obtaining a prior judicial warrant before accessing contents of personal digital devices for purposes of any inquiry or investigation is globally recognised today, permitting warrantless search of digital devices only in the most exceptional of circumstances and often only in cases of searches incidental to arrest.
- RR. BECAUSE absence of a clearly identified investigative purpose at the outset and permitting state agencies to decide what is relevant after they have considered all the material renders the privacy of persons nugatory — any proportionate measure requires that the state clearly define the terms on which it must intrude into the privacy of persons.
- SS. BECAUSE the interest of persons who are not even targets of criminal investigations but mere witnesses would stand on a different footing in need of even greater justifications from the state to support the significant intrusion into the right to privacy which results upon examining the contents of personal digital devices without any limitation.
- TT. BECAUSE the element of proportionality is not only limited to the manner and terms on which state agencies are provided access to personal digital devices, but extends to the manner in which such the contents of

these devices are processed and stored for the purposes of an ongoing inquiry or investigation, and future trial.

UU. BECAUSE a proportionate infringement requires that nothing other than what is relevant to the pursuit of criminal investigations is retained by a state agency upon an examination of a digital device and is accountably stored for purposes of use as evidence in trial, and cannot allow for cloning the complete contents of the device where such copies remain unattended without any measure of security allowing for wanton breaches into one's privacy.

Procedural Safeguards

VV. BECAUSE the significant intrusion into one's privacy resulting from a state agency peering into the contents of personal digital devices requires a robust set of safeguards and cannot operate on the mere say-so or goodwill of the most well-intentioned of officers

WW. BECAUSE the need for procedural safeguards is essential owing to the unique nature of the information at hand — not only are searches of digital devices bound to lead investigators to extremely private and sensitive data about persons, but also such data is infinitely mutable and thus carries a heightened risk of manipulation.

XX. BECAUSE in the absence of any law governing protection of personal data there is an acute need for ensuring sufficient procedural safeguards exist to regulate not only the accessing of personal data by state agencies but also to regulate its processing and deletion, to ensure that the right to privacy is not rendered completely redundant.

- YY. BECAUSE the need to ensure a level of specificity in demands for the information held on personal digital devices made by state agencies requires intervention of a legally trained professional in the form of a judicial magistrate, who functions as the embodiment of this Hon'ble Court's prerogative as the *sentinel qui vive* in respect of ensuring adherence to the rule of law and respect for fundamental rights of persons.
- ZZ. BECAUSE the mere existence of compensatory mechanisms which operate after the fact of a breach having already occurred is insufficient to adequately safeguard the significant privacy interests at stake. Procedural safeguards which trigger only after the breach has occurred are required to be complemented by proactive and preemptive measures to safeguard privacy by limiting the scope and access to digital devices for the hands of state agencies.
- AAA. BECAUSE the inherent and unparalleled mutability of the information stored on digital devices necessitates strong procedural safeguards be put in place to ensure that the integrity of the electronic records accessed for the pursuit of any investigation or inquiry is secured and the persons subject to intrusions of their privacy are not subjected to further harms on account of any manipulation or leakage of their sensitive personal information.
- BBB. BECAUSE a clear process for demanding data deletion or identification of the manner in which seized data is being held renders it incapable for the aggrieved person to be satisfied and be secure in the knowledge that her private information is not prone to misuse or manipulation at the hands of rogue actors within or outside the state machinery.

CCC. Any other grounds that may be raised during oral submissions with the leave of this Hon'ble Court.

65. The Petitioner has not filed in any High Court or the Supreme Court of India on the subject matter of the instant petition.

66. The issues being raised in the present petition are closely connected with the issues raised before this Hon'ble Court in W.P. (Crl.) No. 138 of 2021, titled '*Ram Ramaswamy & Ors. v. Union of India & Ors.*'. This Hon'ble Court was pleased to issue notice in the aforesaid petition to Respondent No. 1 therein *vide* order dated 26.03.2021, and thereafter has been pleased to consider the matter on 26.07.2021, 07.09.2021, and on 05.08.2022, with the next date of hearing tentatively scheduled for 26.09.2022.

PRAYER

In light of the above mentioned facts and circumstances, the Petitioner humbly prays that this Hon'ble Court may:

A. Declare

1. That the contents of an arrested / accused person's digital device and password / passcode / biometric ID thereof are protected by the guarantee against compelled self-incrimination as under Article 20(3) of the Constitution of India.

50

2. That the extant legal regime of search and seizure does not cover the search, seizure and access to contents of an individual's personal digital devices.
 3. In the alternative, declare that to the extent that the extant legal regime does apply to search, seizure, and access to contents of an individual's personal digital devices, it breaches the fundamental right to privacy under the Constitution of India.
- B. Pass appropriate orders directing the Union of India to draft model legislation for enactment by states in respect of search and seizure of digital devices and examination of their contents in consonance with the fundamental rights guaranteed under Part III of the Constitution of India as interpreted by this Hon'ble Court;
- C. Issue appropriate guidelines to fill the lacuna until such time that legislation is passed, including but not limited to the following:
- a. Law enforcement agencies may not seek access to an individual's digital device without applying for and obtaining a prior judicial warrant, except in cases of emergencies, where such a warrant must be sought for - and granted - within 48 hours of the search, failing which the search shall be deemed to be unconstitutional and any material obtained therefrom rendered inadmissible in evidence.

- b. Any application for such a warrant must not be in the nature of a roving and fishing inquiry and must, in specific terms, set out the nature of information that the law enforcement agency expects to find and secure on the device, with reasonable cause for such expectation.
 - c. Any application for such a warrant must demonstrate, to the satisfaction of the judicial magistrate, that it fulfils the proportionality standard under Article 21, including: (i) that it is impossible to obtain the information from other means, and that (ii) state interests are pressing enough to justify the high degree of violation of the right to privacy.
 - d. Investigating agencies must put into place protocols for: (i) safeguard of information so obtained, including safeguards against leaking; (ii) deletion of information once no longer necessary for the investigation, or in any event, at a reasonable period after completion of the investigation, and (iii) preventing law enforcement agencies from sharing data collected from a digital device with any other government agency or department.
- D. Any other order(s) or direction(s) as this Hon'ble Court may deem fit and proper in the interests of justice.

52

AND FOR THIS KINDNESS, THE PETITIONER AS DUTY BOUND
SHALL EVER PRAY

Drafted by:

Filed by:

Filed on:19 .09.2022

(RAHUL NARAYAN)
Advocate of Petitioner