IN THE HIGH COURT OF DELHI AT NEW DELHI

ORIGINAL JURISDICTION

(UNDER ARTICLE 226 OF THE CONSTITUTION OF INDIA)

W.P. (C) NO. OF 2022

IN THE MATTER OF:

SNTHOSTINGS

[redacted]

...PETITIONER

VERSUS

UNION OF INDIA

...RESPONDENT

WRIT PETITION UNDER ARTICLE 226 SEEKING AN APPROPRIATE WRIT, ORDER AND/OR DIRECTION AGAINST DIRECTION (IV) & (V) OF DIRECTIONS DATED 28.04.2022 AND NUMBERED 20(3)/2022-CERT-IN ISSUED BY THE RESPONDENT, VIA THE INDIAN COMPUTER EMERGENCY RESPONSE TEAM

TO,

THE HON'BLE CHIEF JUSTICE

AND HIS COMPANION JUDGES OF THE

HON'BLE HIGH COURT OF DELHI AT NEW DELHI

THE HUMBLE PETITION OF THE PETITIONER ABOVE NAMED:

MOST RESPECTFULLY SHOWETH:

1. The Petitioner, a provider of Virtual Private Network ('**VPN'**) services, is constrained to file the captioned Petition through [redacted] seeking a writ, order, or direction to set aside directions (iv) and (v) of Direction No. 20(3)/2022-CERT-In (collectively referred to as '**Impugned Directions**') dated 28.04.2022, notified by the Respondent through the Indian Computer Emergency Response Team ('**CERT-In**') under Section 70B of the Information Technology Act, 2000 ('**IT Act, 2000**'). Direction No. 20(3)/2022-CERT-In ('**2022 CERT-In Directions'**) requires that in case of any incident, the information collected by Petitioner and other target entities under the Impugned Directions, must be shared with the Respondent; failure to furnish information or non-compliance with the Impugned Direction is punishable with imprisonment of up to one year, or fine, or both under sub-section (7) of Section 70B of the IT Act, 2000.

A true copy of Direction No. 20(3)/2022-CERT-In dated 28.04.2022, passed by the Respondent through CERT-In is annexed herewith as **Annexure P-1**

2. By way of the Impugned Directions, the Respondent has directed a range of entities, including the Petitioner (and other Virtual Private Network providers), to (**a**) mandatorily enable logs of all information and communications technology ("ICT") systems and maintain them securely for a rolling period of 180 days within the Indian jurisdiction ('**Impugned Direction IV'**); and (**b**) register and maintain extremely detailed and invasive personal information of users – such as validated names, address, contact numbers, and email address of subscribers, period of hire, Internet Protocols allotted to members, the purpose of hire and ownership pattern of subscribers – for 5 years or longer, as mandated by law, even after any cancellation or withdrawal of registration of a user ('**Impugned Direction V'**). The Petitioner respectfully submits that the Impugned Directions are *ex facie* contrary to law.

3. The Impugned Directions were to come into effect from 28.06.2022. However, *vide* Direction No. 20(3)/2022-CERT-In dated 27.06.2022, the Respondent *inter alia* extended timelines for enforcement of the 2022 CERT-IN Directions for Micro, Small and Medium Enterprises ('**MSMEs**') such as the Petitioner till 25.09.2022.

   A true copy of Direction No. 20(3)/2022-CERT-In dated 27.06.2022 extending timelines for the enforcement of the Impugned Directions till 25.09.2022 is annexed herewith as **Annexure P-2**.

4. The Petitioner provides Virtual Private Network ('**VPN**') services which enable its users to access the internet semi-anonymously and is nothing short of a public good at a time when cyberspace is rife with dangers to one's liberty, reputation, property, and dignity. By mandating the Petitioner to collect, store and share personally identifiable information of its customers and also make it available to the Respondent and possibly other government agencies in an undetermined array of situations, the Impugned Directions so drastically alter the nature of the service being offered that they effectively prohibit the Petitioner from providing VPN services altogether. In fact, many global players have suspended operations in India owing to the kind of restrictions imposed by the Impugned Directions. The Impugned Directions thus directly implicate the right to carry on trade guaranteed under Article 19(1)(g), and it is submitted that these restrictions on the Petitioner's rights are not reasonable restrictions in the interests of the general public, as required under Article 19(6) of the Constitution of India.

5. Mandating the Petitioner to pervasively monitor user activity and store this data for arbitrarily and unreasonably long periods under the guise of security measures is nothing short of treating the entire class of people who use VPN services as suspects for crimes that have not even been identified yet. This branding of an entire population as a suspect community was distinctly frowned upon by the Hon'ble Supreme Court when it struck down the highly disproportionate data

storage policy initially provided for in the context of the Aadhaar Act, which similarly required data to be stored for over five years. A compliance regime which is narrowly tailored to minimise data collection, processing, and storage is easily achievable and eminently more closely connected to the purported legitimate state object of enhancing cyber-security in the present case, and the Impugned Directions ought to be struck down as being disproportionately invasive of the right to privacy.

6. It is further submitted that the Impugned Directions are *ultra-vires* Section 70B(6) of the IT Act, 2000, and liable to be struck down purely on these grounds.

PARTIES

7. The Petitioner is 'SnTHostings', a sole proprietorship registered under the Maharashtra Shops and Establishment Rules, 2018. It is filing the present Petition through [redacted] The Petitioner was established in 2013 and has its head office in Amegaon Budril, Pune, Maharashtra - 411046. On 05.06.2016, the Petitioner commenced providing services, and after the notification of Maharashtra Shops and Establishment Rules, 2018, duly provided an online intimation of commencing services to the competent authority in accordance with Rule 8 of the said rules.

8. Since commencing business, the Petitioner has provided services such as VPN, Virtual Private Server ('**VPS**'), Remote Desktop Protocol and Dedicated Root Services to over 15,000 customers worldwide through its website, www.snthostings.com. It has over 50 servers in several countries including the United States of America. As detailed below, the Petitioner's customers use these services to browse the internet almost anonymously. Considering the nature of these services, the Petitioner adheres to a strict privacy policy which mandates that the Petitioner collects only such personal information as is voluntarily provided by its customers and to not maintain any logs of the activities of its customers who avail of the Petitioner's VPN, VPS or hosting services. In the past, the Petitioner has provided assistance to law enforcement agencies who have sought specific information regarding its customers.

   A typed copy of the Petitioner's application for intimation under Rule 8 of the Maharashtra Shops and Establishment Rules, 2018 is annexed herewith as **Annexure P-3**.

   A typed copy of the Petitioner's privacy policy, as available on its website https://snthostings.com/privacy-policy/ is annexed herewith as **Annexure P-4**.

   A typed copy of the Petitioner's Terms of Service, as available on its website https://snthostings.com/term-of-service/, is annexed herewith as **Annexure P-5**.

9. The Respondent is the Union of India through Director General, CERT-In. On 19.01.2004, the Union Government established CERT-In under Section 70B of the IT Act, 2000, as a national agency empowered to perform functions listed under Section 70B(4) of the IT Act, 2000. These functions include collecting, analysing, and disseminating information on cyber incidents; forecasting and alerts of cyber security incidents, and; undertaking emergency measures for handling cyber security incidents. Section 70B(6) of the IT Act, 2000 empowers CERT-In to '*call for information and give directions'* to carry out the functions stated in Section 70B(4).

BRIEF STATEMENT OF FACTS

10. The Petitioner has been providing VPN services since 2013. VPNs are a privacy-advancing technology that can be downloaded on any device and are becoming incredibly necessary in the modern age, attaining the status of a public good. VPN services are completely legal and are also provided by public sector telecommunication service providers such as Bharat Sanchar Nigam Limited and Mahanagar Telephone Nigam Limited.

11. When users access the internet without VPNs, they constantly, unknowingly, and often involuntarily, share personal data with other entities on the web, which may include malicious actors and hackers. The personal data accessible to these entities may include a user's

name, address, Internet Protocol ('**IP**') Address, contact information, and other deeply invasive personal information about sexual orientation, political affiliation and financial information such as bank account or credit card or debit card details. This data is used to create profiles of users, which are sold to advertisers or data brokers. This data, if it falls into the wrong hands, could also be used for malicious purposes such as hacking or identity theft.

A report by the Federal Trade Commission of the United States of America, titled '*A look at what ISPs know about you: Examining the privacy practices of six major internet service providers'* dated 21.10.2021, is annexed herewith as **Annexure P-6**.

12. VPNs create a 'secure tunnel' between a user's device and the internet through a series of virtual connections routed online. These virtual connections encrypt data as it travels between one computer and another. As a result, VPN services ensure that the IP addresses of users remain secure and third parties cannot identify a user behind the VPN.

A true copy of an article dated 16.08.2018 by the Centre for Democracy and Technology titled '*Techsplanations: Part 5, Virtual Private Networks'* is annexed herewith as **Annexure P-7**.

A true copy of an image from www.managementhelp.org explaining how VPN services work is annexed herewith as **Annexure P-8**.

13. VPN services provided by the Petitioner thus enable its customers to access the internet without revealing their identity, enabling them to stop the involuntary sharing of personal information with third-party entities. It is pertinent to note that users may well proceed to share such personal information even while using a VPN connection; the critical difference being that in all such cases, they are *actively* choosing to do so. Thus, VPN services facilitate user choice on the internet in an unparalleled manner and are integral to securing the right to privacy online.

14. In 2020, in the wake of the COVID-19 pandemic, the use of VPN services soared tremendously. As businesses moved online from traditional workplaces, they started to rely heavily on VPN service providers, such as the Petitioner, to ensure that data was protected and safe from hacking. In 2021, India witnessed a growth of 671% in downloads of VPN Services. As a result, according to the Global VPN Adoption Index maintained by Atlas VPN, VPN services were downloaded 27 crore times by individuals or businesses based in India.

    A screenshot of the Global VPN Adoption Index for 2021 maintained by Atlas VPN is annexed herewith as **Annexure P-9**.

15. VPN services provided by the Petitioner and other similar entities are among other things used for the following purposes:

a. **Protecting sensitive data:** Governments, corporations, and individuals use VPN to add an additional layer of security to protect their sensitive data. If they do not use VPN, such data would be logged and stored by ISPs and other intermediaries, rendering that data susceptible to cyber-attacks which could potentially put sensitive details in the wrong hands.

b. **Engaging in financial transactions:** VPN services anonymise outgoing traffic by encrypting online activity. This ensures that financial details such as bank account / credit card / debit card details are not accessible to third parties and, thus, furthers cyber security.

c. **Security on public networks:** Individuals often use VPNs while using public networks like those provided at railway stations, airports, hospitals, etc. These public networks are easy to hack because they do not provide the protections provided by private networks. Using a VPN service to tunnel data through a secured network ensures that malicious actors cannot access everything a user does on public networks.

d. **Data privacy from services on the internet:** Search engines, social media platforms, internet service providers and other service providers constantly surveil the activity of users and identify them through IP addresses. Using the information they collect through surveillance, these services target their users with customised advertisements. VPN services hide the IP address of their users and ensure that they are not being monitored. Thus, personal information of users, including name, contact details, sexual orientation, political affiliation and financial information such as bank account or credit card or debit card details, is not accessible to third parties. VPN services are therefore uniquely useful for vulnerable groups such as members of the LGTQIA+ community, civil rights activists, journalists and whistleblowers who could be at risk of physical harm because of data collection and sharing practices of third parties.

16. On 22.05.2015, the United Nations Human Rights Council's Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, recognised the importance of VPNs in their report numbered A/HRC/29/32. The Special Rapporteur observed that anonymity liberates individuals by empowering them to impart ideas or opinions more than they would, using their actual identity. The Rapporteur has stated that using tools such as VPNs, these individuals can ensure full anonymity, including hiding original IP addresses. In the same Report, the Special Rapporteur

recommended that States refrain from making the identification of users a condition for access to digital communication.

A copy of the United Nations Human Rights Council's Special Rapporteur report dated 22.05.2015 and numbered A/HRC/29/32 is annexed herewith and marked as **Annexure P-10**.

17. Considering the purposes for which VPNs are used, the Petitioner adheres to strict privacy policies, which means that it does not collect, store or process its users' data. It also does not maintain data logs, as maintaining a log is similar to the act of keeping a record and it would record all user activity while using the VPN. The information which log files store includes the names of the websites a user visits and even the date, time and duration of such visits. Adhering to strict privacy policies and not storing logs of user activity are standard industry practices for VPN providers globally and are an integral part of such services that customers are paying for. If the Petitioner were to collect, store or process personal data or log user activity as required by the Impugned Directions, there would be no real difference between it and other entities on the internet, such as ISPs or social media intermediaries.

18. On April 28, 2022, Respondent issued the 2022 CERT-In Directions, where specifically the following requirements were imposed:

> *(iv) All service providers, intermediaries, data centres, body corporate and Government organisations shall mandatorily enable logs of all their ICT systems and*

maintain them securely for a rolling period of 180 days and the same shall be maintained within the Indian jurisdiction. These should be provided to CERT-In along with reporting of any incident or when ordered / directed by CERT-In.

(v) Data Centres, Virtual Private Server (VPS) providers, Cloud Service providers and Virtual Private Network Service (VPN Service) providers, shall be required to register the following accurate information which must be maintained by them for a period of 5 years or longer duration as mandated by the law after any cancellation or withdrawal of the registration as the case may be:

a. Validated names of subscribers/customers hiring the services
b. Period of hire including dates
c. IPs allotted to / being used by the members
d. Email address and IP address and time stamp used at the time of registration / on-boarding
e. Purpose for hiring services
f. Validated address and contact numbers
g. Ownership pattern of the subscribers / customers hiring services
....

....

And whereas, in case of any incident, the above-referred entities must furnish the details as called for by CERT-In. The failure to furnish the information or non-compliance with the ibid. directions, may invite punitive action under subsection (7) of the section 70B of the IT Act, 2000 and other laws as applicable.

19. The Impugned Directions are *ultra-vires* Section 70B(6) of IT Act, 2000 as they require Petitioner to collect information it otherwise

would not have collected. Under threat of punitive action, the Impugned Directions require the Petitioner to collect logs which record the activities of the customers as well as personal information of its customers. In violation of the principle of storage limitation, the Petitioner is then mandated to store logs for an arbitrary period of 180 days and store identifiable information of customers for the duration they avail services and a further 5 years or longer even after customers have stopped availing its services. Whilst the Impugned Directions refer to storage as 'mandated by law' there is no law to the best of the Petitioner's knowledge that in fact creates such requirements in the first place. Further, the Impugned Directions authorise the Respondent to direct the Petitioner to hand-over the information it collects. However, they do not impose any limitation on how long the Respondent could store such data, again in violation of the principle of storage limitation. The Respondent is also not prohibited from sharing the data it obtains from the Petitioner with third parties, and thus, customer data could easily be used for purposes entirely unrelated to cyber-security. Thus, while the purported object of the Impugned Directions is to advance cyber-security their implementation clearly results in outcomes that are, in fact, completely contrary to this supposed objective as they unnecessarily cause creation of new databases with unique and previously unavailable private information of persons and thereby increase possible targets for rogue elements to exploit.

20. In view of the above, the Impugned Directions compel the Petitioner to entirely alter the nature of its business and at significant and unreasonable expense in the form of hiring personnel, buying server space, securing personal data from cyber-security threats and obtaining technical know-how. By making it a precondition for doing business that it retains deeply invasive personal data whilst offering VPN services, the Respondent has imposed constraints on the exercise of the Petitioner's Article 19(1)(g) rights that are wholly unreasonable and antithetical to the benefit of the public at large. Consequent to the Impugned Directions there would remain no distinction between services offered by the Petitioner to users as against them browsing the internet without any security. Users would be subject to similar tracking online and susceptible to data manipulation in the event of any breach suffered by not only the Petitioner, but also the many subsequent and undefined recipients of that data owing to its being shared with Respondent and possibly other entities, and retained for several years as well. The Impugned Directions practically render offering VPN services entirely illegal, which is beyond the scope of any reasonable restriction that could be imposed under Article 19(6).

21. On 05.05.2022, the Information Technology Industry Council ('**ITI'**), a body representing multinational technology companies such as Adobe, CISCO, Google and Microsoft, addressed a letter to the Respondent regarding the 2022 CERT-In directions. The Letter

stated that requirements to securely maintain logs of ICT systems for a rolling period of 180 days were '*not a best practice'* and that '*it would make such repositories of logged information a target for global threat actors'*.

A copy of ITI's letter dated 05.05.2022 to the Respondent is annexed herewith as **Annexure P-11**.

22. On 18.05.2022, Respondent released a Frequently Asked Questions ('**FAQ**') document, which according to the Press Information Bureau ('**PIB**'), '*explains the nuances of the Direction numbered No. 20(3)/2022-CERT-In'*. The FAQs, which are not binding legal documents, *inter alia,* state that the 2022 CERT-In Directions do not affect the informational privacy of users as CERT-In will seek information from service providers only in case of cyber-security incidents — which is not borne out from the Directions themselves. In any event, the claim is *ex facie* incorrect, as mandating entities such as the Petitioner to collect invasive personal information of its users violates their informational privacy. Moreover, the 2022 Directions do not provide any safeguards to ensure that the Respondent only uses personal information for stated purposes, and also do not restrict the Respondent from sharing such data with third parties.

A true copy of the FAQ document dated 18.05.2022 is annexed herewith and marked as **Annexure P-12**.

23. Given the Impugned Directions, several major VPN service providers decided to leave India. During June 2022, ExpressVPN, Surfshark, and NordVPN — all global leaders in the market — suspended India operations indefinitely on account of the incompatibility of the Impugned Directions with the essence of what it is to provide VPN Services and their commitment to user privacy and minimising security threats.

    A true copy of the ExpressVPNs blog post dated 02.06.2022, titled '*Rejecting data demands, ExpressVPN removes VPN servers in India'* is annexed herewith as **Annexure P-13**. A true copy of Surfsharks blog post on its website dated 07.06.2022, and titled '*Surfshark shuts down servers in India in response to data law'* is annexed herewith as **Annexure P-14**. A true copy of the blog post dated 20.06.2022, by NordVPN titled '*India orders VPN companies to collect and store user data'* is annexed herewith as **Annexure P-15**.

24. The entities mentioned above could leave India because they are international corporations which can afford to continue providing their services in other jurisdictions. However, for the Petitioner, relocating to another country would be extremely expensive and will drastically undermine the viability of his business. Accordingly, on 10.06.2022, the Petitioner through its Chief Executive Officer addressed a legal representation to Respondent seeking a recall of the Impugned Directions. The Respondent has not replied to this

representation till date but did issue Direction No. 20(3)/2022-CERT-In dated 27.06.2022 to extend timelines for compliance with the Impugned Directions.

A true copy of the Petitioner's representation dated 10.06.2022 is annexed herewith as **Annexure P-16**.

25. Thus, aggrieved by the Impugned Directions, the Petitioner has preferred the present Petition seeking these be set aside on the following, amongst other, grounds.

GROUNDS

Impugned Directions violate the right to carry on any trade or business guaranteed under Article 19(1)(g) of the Constitution and are not saved by Article 19(6)

A. BECAUSE the Petitioner performs an essential public function of providing VPN services. The Petitioner's right to provide such services is protected under Article 19(1)(g). These services are essential as they protect the right to privacy of individuals, businesses and a range of other entities by enabling them to access the internet privately. The Hon'ble Supreme Court in *Central Public Information Officer, Supreme Court* v. *Subhash Chandra Agrawal,* (2020) 5 SCC 481 has held that the right to privacy includes the right to protect anonymity, and stated that anonymity

is where an individual seeks freedom from identification (**Sanjiv Khanna J**, **Para 54**).

B. BECAUSE Impugned Direction IV unreasonably restricts the Petitioner's right to provide VPN services. Customers rely upon the Petitioner's services to access the internet anonymously, but Impugned Direction IV requires Petitioner to maintain a log of every activity of its customers, including the name of the websites they visit and even the date, time and duration of such visits. The Petitioner submits that such invasive tracking is completely antithetical to the notion of VPN services and the Impugned Directions ensure that customers will choose not to avail of the Petitioner's services which entail being monitored on the internet, ultimately driving the Petitioner completely out of business.

C. BECAUSE Impugned Direction V unreasonably restricts the Petitioner's right to provide VPN services by permitting it to provide services only if customers share highly personal information about them and consent for it to be retained for disproportionately long periods. Most individuals or businesses will prefer not to provide these details as they value their privacy, which is the primary reason to turn to VPN services in the first place. Consequently, Impugned Direction V renders the Petitioner's business entirely unviable.

D. BECAUSE the Impugned Directions effectively prohibit VPN services from operating in India. VPN services are attractive to users because of the guarantee that they do not maintain logs or monitor or store the activities of their customers. This guarantee enables users to conduct business securely over the internet. The Impugned Directions force the Petitioner to use its VPN services to monitor the customer activity and obtain and store their personal data.

E. BECAUSE the Impugned Directions are contrary to Article 19(6) of the Constitution for actively contributing to the reduction of service providers and slowly leaving no other players in the market except public sector entities. In fact, the anti-competitive effect of the Impugned Directions has already manifested itself, with the VPN service providers, which have the means to do so, having left India already.

F. BECAUSE the Impugned Directions also impose onerous obligations on the Petitioner, which involve such significant expenditure rendering the Petitioner's business commercially unviable. Impugned Direction IV requires the Petitioner to maintain all logs, including those which do not and cannot provide assistance in responding to cyber-security incidents, and store them for disproportionately long periods of time. Impugned Direction V mandates Petitioner to store the personal data of its customers during the subsistence of their availing services and a

further five years even after they stop availing of services provided by the Petitioner. Complying with these obligations will require the Petitioner to incur significant expenditure in hiring personnel, buying server space, securing personal data from cyber-security threats and obtaining technical know-how. Incurring such expenditure only to comply with regulations will require the Petitioner to wind up its business.

G. BECAUSE the Impugned Directions cannot be saved by Article 19(6) of the Constitution. As stated above, the Impugned Directions impose restrictions which effectively amount to a prohibition. It is a settled position of law that any restriction if amounting to prohibition must satisfy the test that a lesser alternative would be inadequate [*State of Gujarat* v. *Mirzapur Moti Kureshi Kassab Jamat,* (2005) 8 SCC 534 (Para 75)]. The Respondent has to satisfy this Hon'ble Court on why mandating the Petitioner to collect and store data of its customers is necessary to respond to cyber-security incidents, and why the same end could not be achieved by seeking data regarding specific individuals with prior permission from courts akin to a warrant.

H. BECAUSE the Impugned Directions are not in the interest of the general public as they undermine the right to privacy as detailed below, and prohibit the general public from accessing the internet securely as mentioned above. VPN services enable individuals to protect themselves online which is an essential function in an age

where individuals are constantly profiled based on their activities over the internet. VPNs are particularly necessary in India which does not have any law which regulates capturing and processing of personal data. By effectively prohibiting VPN services, the Impugned Directions unequivocally affect the interests of the general public in an adverse manner.

Impugned Directions violate the right to privacy and do not comply with the principles of storage and purpose limitation.

I. BECAUSE the Hon'ble Supreme Court in *Justice K.S. Puttaswamy (Retd.) & Anr.* v. *Union of India.,* (2017) 10 SCC 1 (‘***Puttaswamy - I’)*** includes - a) informational privacy; b) communication privacy; c) anonymity and d) intellectual privacy (**Chandrachud J, Para 250**). Impugned Direction IV *prima facie* violates the right of informational and intellectual privacy of persons using the Petitioner's services by mandating the Petitioner to keep a record of every activity of its customer on the internet. Impugned Direction V also *prima facie* violates the right to anonymity by compelling the Petitioner to identify its customers before providing them services.

J. BECAUSE the data collected pursuant to the Impugned Directions, taken as a whole, could allow for precise conclusions to be made regarding the private lives of the persons whose data has been retained, such as habits, places of residence, social relationships and the place they visit, by not only rogue actors

which may gain access to this trove of information illegally but even by virtue of unrestricted sharing and processing of this data with state agencies as is presently permitted under the Impugned Directions.

K. BECAUSE the Hon'ble Supreme Court in both, *Puttaswamy - I* (**Kaul J, Para 632)** and *Puttaswamy - II* (**Sikri J, Para 158**) held that any restriction on the right to privacy must pass the test of proportionality. The majority in *Puttaswamy - II* (**Sikri J, Para 221)** also held that the state could successfully discharge the burden of proportionality while affecting the privacy rights of citizens by complying with the principles of storage and purpose limitation, and data minimisation. The Impugned Directions do not comply with any of these principles and thus disproportionately violate the right to privacy.

L. BECAUSE the principle of storage limitation requires personal data to be kept only as long as it is necessary [*Puttawamy-II* (**Sikri J, Para 201.4**)]. In *Puttaswamy II,* the Hon'ble Supreme Court of India struck down Regulation 27(1) of the Aadhaar (Authentication) Regulation, 2016 on the grounds that it permitted UIDAI to archive authentication transactions data for 5 years. The Supreme Court ruled that the regulation in question '*severely affected'* the citizen's right to erasure of data and thus, should not be retained for more than six months (**Sikri J, Para 240**). Impugned Directions raise similar concerns by requiring Petitioner

to retain personal data for an arbitrary period in excess of five years, and by practically permitting the Respondent to retain such data for an indefinite period.

M. BECAUSE Impugned Direction IV requires the Petitioner to retain the logs of the activities of its customers for an arbitrary period of 180 days and provide them to the Respondent on demand. Impugned Direction V similarly requires the Petitioner to retain the personal information of its customers during the period of their availing services, and for an arbitrary period of 5 years after the customers have stopped availing of the services provided by the Petitioner, and provide such data to the Respondent in the event of a cyber-security incident. In both cases, if the Respondent obtains data from Petitioner and other similar entities, it could retain it for an indefinite period, even after data has served the purpose for which it was taken. This is in complete disregard of the principle of storage limitation and disproportionately violates the right to privacy.

N. BECAUSE the Impugned Directions also do not comply with the principle of purpose limitation. Purpose limitation requires that personal data collected and processed by data controllers should be relevant to the purpose for which it is processed. Impugned Direction IV requires Petitioner to collect logs of every user, including those without any connection with cyber-security incidents. Moreover, the nature of logs directed to be collected is

not limited to those that may assist the Respondent in investigating cyber-security incidents. Thus, Impugned Direction IV requires the collection of data which is not at all relevant to the purpose for which it is collected. Similarly, Impugned Direction V requires Petitioner to collect personal details of every customer, presuming all of them to be cyber-criminals and violating the principle of purpose limitation.

O. BECAUSE the Respondent could have issued *less restrictive* directions which would have complied with the principle of purpose limitation and would bear a closer nexus with the purported state object of enhancing cyber-security. For instance, directions to entities such as the Petitioner to maintain logs of a specific user on a case-by-case basis, based on a reasonable suspicion recorded in writing that the said user may be using VPN services to threaten cyber-security, would achieve the same purpose in a manner without jeopardising the privacy of all users and inflicting the Petitioner with unsustainable costs. However, the Impugned Directions have instead presumed every user of VPN services to be criminals and unconstitutionally directed the Petitioner to maintain a record of their activities in complete violation of the principle of purpose limitation.

P. BECAUSE in *Puttaswamy - II* (**Sikri J, Para 216**), the Hon'ble Supreme Court noted with approval the Court of Justice of European Union's decision in *Tele2 Sverige AB* v. *Post-Och*

Telestyrelsen, 2017 QB 771. In that case, CJEU struck down a provision which required providers of electronic communication services to retain the name, address, telephone number and IP address of their subscribers for the purpose of fighting crime. CJEU held that legislation did not comply with purpose limitation as it collected data of '*all persons using electronic communication services, even though those persons are not, even indirectly, in a situation that is liable to give rise to criminal proceedings'* **(Para 105**). The Impugned Directions similarly require retention of data of individuals who do not have any link with cyber-security incidents.

Q. BECAUSE the Hon'ble Supreme Court in *Puttaswamy II* struck down a provision which mandated the linkage of bank accounts with Aadhaar cards while stating that '*under the garb of prevention of money-laundering or black money, there cannot be such a sweeping provision which targets every resident of the country as a suspicious person. Presumption of criminality is treated as disproportionate and arbitrary'* (**Sikri J, Para 430**). The Impugned Directions similarly carry a presumption of criminality as they require the Petitioner and other entities to collect data of every customer, and thus, do not distinguish between *bona fide* users and those who may be using these services for unlawful purposes.

R. BECAUSE the a High Court in England in *Davis* v. *Home Secretary,* CO/3665/2014 held that Section 1 of the United Kingdom's Data Retention and Investigatory Powers Act 2014 was inconsistent with the guarantee of the right to privacy. The Court observed that the provision permitted the executive to direct public communication operators such as ISPs to provide personal information of their users to the Government without laying down precise rules which would ensure that only such data is collected and provided, which is strictly restricted to the purpose of preventing and detecting precisely defined serious offences. The Impugned Directions similarly do not contain criteria which would restrict the collection and processing of data only for the purposes of investigating or responding to cyber-incidents.

S. BECAUSE the Impugned Directions also violate the principle of purpose limitation by not restricting the Respondent from sharing the data it collects with third parties or with other governmental agencies. As a result, the data collected by the Petitioner because of the Impugned Directions could easily be used for purposes other than responding to cyber-incidents, and the data principals will not have any recourse against such misuse.

T. BECAUSE it is not necessary for the Respondent to collect personal data of users such as their email addresses, addresses, contact numbers, ownership pattern and the purpose of hiring, to respond to cyber-security incidents. In fact, even the Incident

Reporting Form which is used by service providers to report cyber-security incidents to the Respondent does not require such information. The Respondent has not explained why the personal information of users is necessary to respond to cyber-security, how such information was lacking before the Impugned Directions and why the availability of the information will enable them to respond to cyber-security incidents in a better manner. The burden is on the Respondent to demonstrate the suitability of the Impugned Directions to this Hon'ble Court.

A copy of the Incident Reporting Form as available on the website of the Respondent is annexed herewith as **Annexure P-17**.

Impugned Directions are ultra vires the Section 70B of the IT Act, 2000

U. BECAUSE it is a settled law that any executive action under a statute must be within the confines of the power conferred by that statute. The CERT-In 2022 Directions have been purportedly issued under Section 70B(6) of the IT Act, 2000. The said provision empowers the Respondent to '*call of information and give directions'* to service providers for carrying out functions provided in Section 70B(4). However, the Impugned Directions mandate the Petitioner to collect and maintain data that it would not have collected otherwise. Sections 70B(4) and 70B(6) have been reproduced below:

> *"(4) The Indian Computer Emergency Response Team shall serve as the national agency for performing the following functions in the area of cyber security –*
> *(a) collection, analysis and dissemination of information on cyber incidents;*
> *(b) forecast and alerts of cyber security incidents;*
> *(c) emergency measures for handling cyber security incidents;*
> *(d) coordination of cyber incidents response activities;*
> *(e) issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, preventation, response and reporting of cyber incidents;*
> *(f) such other functions relating to cyber security as may be prescribed.*
>
> ..
>
> *(6) For carrying out the provisions of sub-section (4), the agency referred to in sub-section (1) may call for information and give direction to the service providers, intermediaries, data centres, body corporate and any other person."*

V. BECAUSE Sections 70B(4) and 70B(6) only permit the Respondent to direct companies to provide the information they maintain in the usual course of business. However, the Impugned Directions mandate the Petitioner not only to provide information but also to continuously collect and store sensitive personal and invasive information of its users, which the Petitioner would not have otherwise collected.

W. BECAUSE the Impugned Directions undermine the Respondent's function of handling cyber-security incidents by mandating the Petitioner to collect users' personal data. The storage of such

extensive personal data makes the Petitioner and other similar entities, more susceptible to cyber-security attacks. The principle of data minimisation, i.e. collection of only necessary data and deletion of data once the purpose for which it has been collected, substantially reduces the possibility of breach of personal data through cyber-security attacks. The Impugned Directions violate the principle of data minimisation by mandating the collection of personal data and thus undermine the function of the Respondent to handle cyber-security incidents. Therefore, the Impugned Directions are *ultra-vires* IT Act, 2000 as they cannot carry out the functions stated in Section 70B(4).

X. BECAUSE the Impugned Directions are in the nature of essential legislative functions, which can only be authorised by the Parliament and not agencies of the Union Government such as the Respondent. [*In re Delhi Laws Act, 1912* 1951 SCR 747 (**Para 311**)]. If such functions are exercised by bodies other than the Parliament, such actions are unconstitutional. The Impugned Directions require the Petitioner to collect and retain vast amounts of personal data, which *prima facie* infringes the right to privacy. In absence of the Impugned Directions, the Petitioner had no occasion to collect such data. It is submitted that introducing limits on fundamental rights is the very definition of 'core legislative function', which cannot be delegated to the executive decree. Thus, to mandate service providers to collect such vast amounts of

data and to log the activities of their users, there must be a clear legislative policy imposed through a statute enacted by a Parliament. The Respondent cannot, by way of a notification, issue directions which do not even find a place in the IT Act, 2000.

Y. BECAUSE Respondent has directed service providers to collect and maintain massive amounts of data and surveil citizens solely based on an executive direction. It is settled law per *State of Madhya Pradesh v. Thakur Bharat Singh*, 1967 (2) SCR 454 (Para 5), that all executive action, which operates to the prejudice of any person, must be supported by the authority of law. It is also a settled position of law, as per the *State of UP vs Johri Mal*, (2004) 4 SCC 714 that executive actions do not carry the same status as a statute since they can be "*amended, altered or withdrawn at the whims and caprice of the executive for the party in power*" and thus, the law cannot be substituted by the executive which may be subject to administrative vagaries.

Z. And any other grounds that may be added, as appropriate, with the leave of this Hon'ble Court.

26. The Petitioner submits that the Respondent is situated in New Delhi, which is within the territorial jurisdiction of this Hon'ble Court. Moreover, the Respondent issued the Impugned Directions in Delhi on 28.04.20222. The Petitioner, therefore, submits that this Hon'ble Court has the jurisdiction to entertain and try this Petition.

27. The Petitioner submits that he does not have any other alternative efficacious remedy, and that he has exhausted all remedies available to him

28. The Petitioner has not filed any other Petition concerning the subject matter of this Petition either in this Hon'ble Court or any other forum.

PRAYER

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

A. Issue a writ order or direction to set aside direction (iv) and (v) of Direction No. 20(3)/2022-CERT-In dated April 28, 2022 issued by the Indian Computer Emergency Response Team; and

B. Pass any other order (s) or relief (s) as this Hon'ble Court may deem fit.

PETITIONER

[redacted]

THROUGH

[redacted]

VRINDA BHANDARI, ABHINAV SEKHRI,

TANMAY SINGH, KRISHNESH BAPAT, ANANDITA MISHRA, NATASHA MAHESHWARI & MADHAV AGGARWAL

ADVOCATES FOR THE PETITIONER

[redacted]

DATE: 15.09.2022
PLACE: NEW DELHI