IN THE HON'BLE HIGH COURT OF DELHI AT NEW DELHI

WRIT PETITION (CIVIL) No. 13997 OF 2022

IN THE MATTER OF:

M/S SNT HOSTINGS **... PETITIONER**

VERSUS

UNION OF INDIA **... RESPONDENT**

INDEX

S. No.	Particulars	Page No.
1.	Counter Affidavit on behalf of the Respondent	1-25
2.	**Annexure – R1** True copy of the said Notification dated 27.10.2009.	26-27
3.	**Annexure – R2 (Colly)** Screenshots of the Petitioner's website and app stores.	28-67
4.	**Annexure – R3** Article posted by the Petitioner on its website.	68-77
5.	Proof of Service	78

Respondent

Through

[redacted]

Vaibhav Gaggar, Advocate

[redacted]

Date: 05.12.2022

Place: New Delhi

IN THE HON'BLE HIGH COURT OF DELHI AT NEW DELHI

WRIT PETITION (CIVIL) No. 13997 OF 2022

IN THE MATTER OF:

M/S SNT HOSTINGS **... PETITIONER**

VERSUS

UNION OF INDIA **... RESPONDENT**

COUNTER AFFIDAVIT ON BEHALF OF THE RESPONDENT (DIRECTOR GENERAL, INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-In), MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA)

[redacted]

I. I am duly authorized and competent to affirm this affidavit in my official capacity on behalf of the Respondent. That having gone through the Petition and having perused the same and having made myself conversant with the facts and circumstances of the present case on the basis of official records, I am able to depose on oath and file this affidavit.

PRELIMINARY SUBMISSIONS:

2. Digital technology and usage of internet has grown exponentially and has become integral part of modern life, spanning into almost all sectors pervasively. At the same time, this advancement of technology has increased the attack surface, thereby opening up vulnerabilities for exploitation by the malicious actors.

3. The Petitioner itself has admitted that cyberspace is rife with dangers to one's liberty, reputation, property and dignity, therefore, the stated danger also exists before this country as a sovereign society at large as well. The total anonymity of state and non-state actors and rogue elements to operate on internet or in cyber space may cause havoc with their nefarious activities. Further, the identification and apprehension of offenders indulging in crimes committed by using computer resource is also next to impossible if suitable and proportionate safeguards are not put in place in this regard. In view of the same, the Respondent has issued Cyber Security Directions dated 28.04.2022 (hereinafter referred to as **"Cyber Security Directions"**), in order to enhance the safety and security of citizens of India on the internet/cyber space. The relevant extract of the Cyber Security Directions, has been reproduced herein below:

> ***"And whereas**, it is considered expedient in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence using computer resource or for handling of any cyber incident, that following directions are issued to augment and strengthen the cyber security in the country:*
>
> ***(i)** All service providers, intermediaries, data centres, body corporate and Government organisations shall connect to the Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP servers traceable to these NTP servers, for synchronisation of all their ICT systems clocks. Entities having ICT infrastructure spanning multiple geographies may also use accurate and standard time source other than NPL and NIC, however it is to be ensured that their time source shall not deviate from NPL and NIC.*
>
> ***(ii)** Any service provider, intermediary, data centre, body corporate and Government organisation shall mandatorily report cyber incidents as mentioned in Annexure I to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents. The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800- 11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents is also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time.*

(iii) *When required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents, the service provider/intermediary/data centre/body corporate is mandated to take action or provide information or any such assistance to CERT-In, which may contribute towards cyber security mitigation actions and enhanced cyber security situational awareness. The order / direction may include the format of the information that is required (up to and including near real-time), and a specified timeframe in which it is required, which should be adhered to and compliance provided to CERT-In, else it would be treated as non-compliance of this direction. The service providers, intermediaries, data centres, body corporate and Government organisations shall designate a Point of Contact to interface with CERT-In. The Information relating to a Point of Contact shall be sent to CERT-In in the format specified at Annexure II and shall be updated from time to time. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact.*

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*"

4. A conjoint, comprehensive and holistic reading of the above said cyber security directions evinces that the same have been issued for preventing incitement to the commission of any cognizable offence using computer resource or for handling of any cyber incident, and to augment and strengthen the cyber security in the country. However, instead of duly complying with the said Cyber Security Directions, the Petitioner herein has challenged the directions (iv) and (v) of the Respondents' directions issued on 28th April 2022 (hereinafter referred to as the **"impugned directions**") as being ultra-vires.

NOTARY R.V. SINGH Advocate Regd. No. 22282 GOVT. OF INDIA

5. It is submitted that the whole basis of the Petitioner's arguments appears to be that VPNs are becoming incredibly necessary in the modern age, attaining the status of a public good. However, the reality is that the VPN Services, which are basically Internet–proxy like services, are highly prone to misuse, since the offenders cannot be traced in a timely manner, if at all.

6. Admittedly, with the onset of COVID-19, companies increasingly adopted Work from Home (WFH) to continue to conduct their operation but companies use Corporate VPN to enable such Work from Home which are distinct from "Internet-proxy" like VPN Services, as allegedly provided by the Petitioner. It is pertinent to note that the impugned direction number (v) regarding registering and maintaining subscribers/customers information is not applicable to corporate VPNs but the direction no.(iv) is applicable to all service providers, intermediaries, data centres, body corporate and Government Organisations.

7. The Petitioner has further stated that a user accessing internet without VPNs often involuntary shares personal data with other entities on web. However, the fact is that a user accessing internet through VPN Services or otherwise, shares personal data due to lack of awareness, or due to acting in negligent manner, or due to some inducement or even on voluntary basis etc.

8. VPN Services do not assure or provide infallible or impregnable safety to data fiduciaries. If an ISP can see the activities of user, then VPN service provider may also see on their peril. There are reports that VPN Services have also been found to be indulging in collection of variety of logs. Some VPN Service Providers even monetize on the users' browsing data very similar to what they claim to protect against.

NOTARY R.V. SINGH Advocate Regn.No.2282 Commission Expires on 24-10-2027 Area-Delhi GOVT. OF INDIA

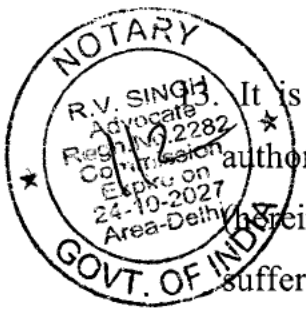
9. There are reports providing that the use of VPN services is not uniformly acceptable across all the nations in the world. The use of VPN services is illegal in certain countries like Iraq etc.; and is highly regulated/restricted in countries like

UAE , Russia etc., whereby it is mandatory for VPN providers to keep all connection logs.

10. It is submitted that the impugned directions in no way prohibit the provision of VPN services but only mandate measured and proportional safeguards which are essential for public good, due to Internet-proxy like VPNs' proneness for misuse.

11. The total anonymity of VPNs may provide some sort of protection but at the same time, it is equally prone to misuse. The balance of individual interest vis-a-vis society's interest ought to be maintained, therefore, the impugned directions per se do not mandate sharing of data with the Respondent unless there is a case of cyber incident. Further, impugned directions mandate Service Providers to only collect basic essential details of users, which is not sensitive information so that in case of any cyber incident, the relevant information is available to analyse the cyber incident.

12. The impugned directions do not mandate the Petitioner with the task of monitoring the activities of its users. The Petitioner is required to keep the security related logs and it is emphatically submitted that the privacy of individuals not affected by these Cyber Security Directions, as it does not require VPN Service providers to make any architectural change nor it requires them to weaken the security (encryption, authentication etc.) in any way. The nature of information required to be collected by service providers includes basic identity related information like name, addresses etc., which is not sensitive in nature.



13. It is submitted that the impugned directions have been issued by a statutory authority established under Section 70B of the Information Technology Act, 2000 (hereinafter referred to as the **"IT Act"**) i.e., the Respondent herein, and do not suffer from any excessive delegated legislation. Section 70B of the IT Act is reproduced herein below:

" 70B. Indian Computer Emergency Response Team to serve as national agency for incident response.–(1) The Central Government shall, by notification in the Official Gazette, appoint an agency of the Government to be called the Indian Computer Emergency Response Team.
(2) The Central Government shall provide the agency referred to in sub-section (1) with a Director General and such other officers and employees as may be prescribed.
(3) The salary and allowances and terms and conditions of the Director-General and other officers and employees shall be such as may be prescribed.
(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.
(5) The manner of performing functions and duties of the agency referred to in sub-section (1) shall be such 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.
(7) Any service provider, intermediaries, data centres, body corporate or person who fails to provide the information called for or comply with the direction under sub-section (6), shall be punishable with imprisonment for a term which may extend to one year or with fine which may extend to one lakh rupees or with both.
(8) No court shall take cognizance of any offence under this section, except on a complaint made by an officer authorised in this behalf by the agency referred to in sub-section (1).]"

14. A conjoint reading of sub-sections (4) and (6) of Section 70B clearly evinces that the Respondent has full authority to issue directions in order to carry out the avowed purpose underlined in sub section 4.

15. Furthermore, it is submitted that the right to practice any profession, or carry on any occupation, trade etc. provided under Article 19(1)(g) of the Constitution is not absolute and is subject to the interest of general public. It is incontrovertible that enhancement of cyber security, in order to make the internet a safe, secure and trusted space for the public clearly falls within the ambit of "public interest". Nevertheless, these impugned directions do not even impose any restriction at all, as the Petitioner can continue to provide its services as these impugned directions are neither prohibitive in nature, nor limiting the business activity of the Petitioner in any manner with regard to access, size; quantum etc.

NOTARY R.V. SINGH Advocate Regn. No. 2282 Commission Expire on 24-10-2027 Area-Delhi GOVT. OF INDIA

16. In the present case, the objective of collection and maintenance of basic identifiable subscriber/customer information and logs of ICT systems at the end the respective entities by themselves and not by the Respondent, is to prevent the commission of cybercrimes and analysis of cyber incidents, thereby enhancing the safety and security of the cyber space. Further, the impugned directions do not have a disproportionate impact because the purpose limitation and retention of data is not being done for merely authentication purposes, which is why the data retention period of 7 years was struck down by the Hon'ble Supreme Court in ***K. S. Puttaswamy and Another v. Union of India (2019) 1 SCC 1 [Puttaswamy II].***

17. It need not be dilated upon that such cyber incidents, cybercrimes/economic offences are complicated and are scattered over a long period of time; and may be done in a staggered manner, in order to avoid any detection, which is why retention of data for a particular duration of time, as mandated by the impugned directions is necessary.

18. Furthermore, the Petitioner, who is not even a user of VPN services, but a company claiming to be providing said VPN services to users, under the guise of taking up cudgels for said VPN users has made the unwarranted allegation that the impugned directions has been done as a surveillance measure.

19. It is submitted that the word surveillance envisages constant/consistent monitoring of activities of a person/entity, which is clearly not the case in the present matter, since the impugned directions only mandate collection and storage of data for a particular interval of time by the entities themselves and user specific information will only be shared by the entities with the Respondent as and when required, in order to analyse cyber incident or cyber security incidents.

20. The data or information sought to be collected as per the impugned directions is required to be shared with Respondent only in the contingencies of cyber incident

or cyber security incident, as per the mandate enunciated in the provisions of section 70B of the IT Act.

21. Furthermore, in view of the Hon'ble Court's decisions in ***K. S. Puttaswamy and Another v. Union of India and Others (2017) 10 SCC 1 [Puttaswamy I]*** and ***Puttuswamy II (Supra)***, even the right to privacy is not absolute and is subject to reasonable restrictions and that provisos to various fundamental rights are an obvious restriction to the right to privacy. It is further submitted that under no circumstances anonymity can be a ground for evasion from lawful authorities or for non-compliance with law.

22. It is further submitted that the Petitioner's understanding of the ***Puttaswamy judgments (Supra)*** is fundamentally flawed and highly misplaced. That in the garb of privacy, the doctrine of proportionality cannot be used to pervert and subjugate security interests and public safety.

23. The doctrine of proportionality as envisaged in the ***Puttaswamy II (Supra)*** judgment consists of the following 4 stages:

(*a*) A measure restricting a right must have a legitimate goal (legitimate goal stage).

(*b*) It must be a suitable means of furthering this goal (suitability or rational connection stage).

(*c*) There must not be any less restrictive but equally effective alternative (necessity stage).

(*d*) The measure must not have a disproportionate impact on the right-holder (balancing stage).

NOTARY R.V. SINGH Advocate Regn No. 2282 Commission Expire on 24-10-2027 Area-Delhi GOVT. OF INDIA

24. The four sub components for a measure for a restriction on a fundamental right to be proportional is not attracted or applicable herein. The measures enunciated in the cyber security directions no. (iv) and (v) to enhance cyber security is not amounting to unreasonable restriction as the directions has a legitimate, precise, compelling goal of analysis of cyber incidents or cyber security incidents such as

ransomware; data breaches; compromising of critical systems etc., besides preventing cyber-crimes like child pornography, financial crimes, terrorism etc.

25. Secondly, the means of retention of data by a VPN Service provider and not by the State itself is a suitable means of furthering this goal and also evinces the bona fide interests of the Respondent.

26. Further, while seeking the impugned directions to be set aside by way of the present petition, the Petitioner itself has not suggested/put forth/contemplated any other equally effective alternative.

27. Furthermore, the solemn and avowed object of preventing cyber incidents and thereby promoting cyber security cannot be relegated to suit the commercial interests of entities like the Petitioner herein. The Petitioner, in order to advance its own financial concerns, is willing to waylay legitimate safety and security interests of the state, in general, and the people, in particular.

28. Further, it is submitted that one of the main arguments of the Petitioner, as noticed in this Hon'ble Court's order dated 28.09.2022, is that the impugned directions are vague and need to be struck down, as held in ***Shreya Singhal v. Union of India (2015) 5 SCC 1.***

29. The Hon'ble Court in ***Shreya Singhal (Supra)***, declared Section 66A of the IT Act vague, for it created an offence without clearly defining the standards of guilt while creating the said offence, as the same was contrary to settled principles of criminal law. The Hon'ble Apex Court further elaborated that open ended and undefined offences, without specifying ingredients offends the basic tenets of criminal law.

30. Thus, since it is no one's case that the impugned directions are creating or defining an offence, the ratio decidendi of ***Shreya Singhal (Supra)*** would not apply to the

NOTARY R.V. SINGH Advocate Regn No. 2282 Commission Expire on 24-10-2027 Area-Delhi GOVT. OF INDIA

present case as the impugned directions are just a methodology to prevent offences and aid in analysis of cyber incidents or cyber security incidents.

31. Furthermore, it belies logic that the Petitioner would share information with the Respondent even on Court orders, if the Petitioner does not collect personal identifiable information of its users, or their logs, in the first place. The Petitioner's suggestion that in order to respond to cyber security incidents, data can be collected by seeking data regarding specific individuals with prior permission from courts akin to a warrant is highly impractical, and would defeat the whole purpose of the timely mitigation of cyber security threats.

32. The Petitioner's contention that the impugned directions should be 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 is highly implausible and frivolous.

REPLY ON MERITS:

I. <u>Impugned Directions have been issued by a Statutory Authority under Section 70B of the IT Act.</u>

1. It is submitted that the Respondent is the "Indian Computer Emergency Response Team (CERT-In)", which is a statutory authority established by the Union of India through the Ministry of Electronics and Information Technology, vide a Notification dated 27.10.2009 under the provisions of Section 70B (1) of the IT Act. A True copy of the said Notification dated 27.10.2009 has been annexed herewith as **ANNEXURE-R1.**

2. That the Respondent has been established to serve as the national agency to perform the following functions in the area of cyber security, as enunciated in sub-section (4) of Section 70B of the IT Act:

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 whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;
f. such other functions relating to cyber security as may be prescribed.

3. It is submitted that during the last four years, the Respondent has either tracked or has received reports about various cyber incidents and cyber security incidents ranging from phishing; ransom ware; distributed denial of service; malware; website intrusion etc. on the internet. A tabular representation of the number of such cyber incidents and cyber security incidents encountered by the Respondent has been enumerated herein below:

Year	**Numbers of cyber incidents or cyber security incidents**
2019	3,94,499
2020	11,58,208
2021	14,02,809
2022 (upto September)	10,19,180

4. That while coordinating response activities as well as emergency measures with respect to the above-mentioned cyber incidents and cyber security incidents from time to time, it has been observed that the requisite information is either not readily available with service providers/data centres/body corporate or not available at all. The said requisite information, which forms part of primary evidence, is absolutely essential for the Respondent to carry out the analysis, coordination and investigation, and in order to effectively handle such cyber security incidents. The

NOTARY R. SINGH Advocate Reg. No. 2282 Commission Expires on 24-[illegible]-2027 Area-Delhi GOVT. OF INDIA

non-availability of such information hinders with the Respondent's statutory obligations to effectively handle and curb cyber security incidents.

5. In order to address the issue of non-availability of data, which obstructs the Respondent's timely and effective response to cyber security incidents, draft cyber security directions were prepared by the Respondent, under the aegis of the Ministry of Electronics and Information Technology in February, 2022 and a consultation with the relevant industry experts was duly conducted in March, 2022, with representatives from Government, IT and Telecom Industry (Global and Domestic), Legal Advisory firms etc. After incorporating the views and suggestions of the said experts, the Cyber Security Directions were issued by the by Respondent in exercise of its statutory powers under sub-section (6) of section 70B of the IT Act, 2000.

6. That the said Cyber Security Directions were issued to augment and strengthen the cyber security in the country as it was considered expedient in the interest of the sovereignty or integrity of India, defence of India, security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence using computer resource or for handling of any cyber incident.

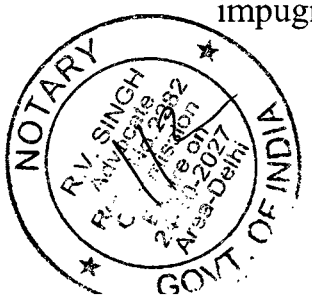
7. The said Cyber Security Directions are intended to ensure timely reporting of cyber incidents to the Respondent, supplemented by necessary information required for analysis of such incidents, mitigation of cyber security incidents/attacks and coordinated incident response measures, thereby ensuring protection in terms of confidentiality and integrity of data/information and availability of services to citizens. Furthermore, the cyber security directions have been issued with the aim of enhancing overall cyber security posture of the country and ensure open, safe, trusted and accountable Internet.

8. It is submitted that personally identifiable information is sine qua non for analysis of cyber security incident or cyber incident; and also for investigation and apprehension of offences in the cases of cybercrime or crimes committed while using computer resource. Therefore, the said cyber security directions are serving the larger public interest.

9. It is further submitted that in order to bring clarity and ensure compliance of the impugned directions, a set of FAQs dated 18.05.2022 were published by the Respondent. Thereafter, another consultation meeting with Industry stakeholders were held on 10.06.2022 to allay the concerns and to clarify the queries of the said stakeholders.

10. After receiving multiple requests from various MSMEs and other organisation, the Respondent on 27.06.2022, extended the timelines for enforcement of impugned directions for MSMEs, by 90 days, in order to enable them to prepare for compliance as per the concerns voiced to Respondent, thereby making the cyber security directions effective from 25.09.2022. It is pertinent to note herein that the Petitioner has claimed to be an MSME and has benefited from the said extension of timelines but instead of preparing for compliance, has challenged the impugned directions on frivolous; false and unfounded notions which depict that Petitioner has no intention to strengthen the cyber security posture of the Country.

11. It is submitted that collection and retention of basic identity information from the subscribers/customers or retention of security related logs does not alter the nature of VPN services or user experience at all and both the things are unrelated and there is no substance in the contention of the Petitioner that Users would be subject to similar tracking online and susceptible to data manipulation in the event of any breach. The fact is that data breach itself constitutes a cyber-incident or cyber security incident, which per se is obligatory to be reported to Respondent and impugned directions are only aimed at strengthening the cyber security.



12. It is submitted that only the unscrupulous elements may be wary or wavering in providing the basis identity information. These impugned directions have not imposed any restrictions at all on the Petitioner; and the Petitioner is free to carry on it trade as these impugned directions do not forbid or prohibit the use of VPN services.

13. That the impugned directions have been issued in exercise of statutory powers bestowed upon the Respondent under section 70B (6) of the IT Act, which are neither prohibitive in nature nor limiting the business activity of the Petitioner in any manner with regard to access, size; quantum etc. The Petitioner is free to carry on its business activities in compliance with these directions and these directions do not impose any restrictions at all.

14. It is trite in law that the word "public interest" under Article 19(6) is of a wide import and includes public security within its ambit. Thus, it is submitted that since the said Cyber Security Directions have been issued to augment and enhance the cyber security of the citizens on the internet, the Petitioner's fundamental right to carry on any occupation/trade/business is in no manner being infringed or violated.

15. In order to have overall glimpse on the reporting of cyber security incidents to Respondent after impugned directions, it has been noted that there has been a rise to the tune of 51% in monthly average, in the reported cyber incidents during the period from July 22 to September 2022 in comparison with the period from January 22 to June 2022.

II. Present petition is nothing but a proxy litigation filed in furtherance of non-bonafide purpose.

16. It is submitted that the invocation of writ jurisdiction by the Petitioner is a ploy to frustrate the Respondent's endeavour to improve the cyber security posture of the country; and that the present petition appears to be nothing but a proxy litigation

initiated at the behest of certain interests to scuttle these directions for vexatious purposes.

17. It is further submitted that Petitioner, has espoused the cause of certain entities such as Express VPN, NORDVPN and Surfshark, stating that these entities have been provided an unfair and unconstitutional choice, while assailing the impugned directions. The fact is that these entities are not entitled to invoke the constitutional legal remedies which are otherwise available to Petitioner, as the writ petition has been filed invoking the provisions of Article 226, alleging infringement of Article 19(1)(g) of the Constitution of India, which guarantees to all the citizens the right to practise any profession, or to carry on any occupation, trade or business, subject to provisions of Article 19(6); and that this legal or remedial window is not available to non-citizens of this country.

18. It is submitted that the Petitioner claims to be engaged in the business of providing Virtual Private Network (VPN) services but upon a perusal of the website of the petitioner, i.e., "www.snthostings.com", it is observed that there is no mention of the "VPN Services" as any of the offerings and that there is also no VPN Service Application available with the name of SnTHosting either on prominent App Stores or on website of the Petitioner. (The screenshots of the Petitioner's website and app stores are annexed herewith as **ANNEXURE-R2 (Colly)**). Hence, the claim of Petitioner is required to be tested on probative value. On the contrary, it appears that, the Petitioner is primarily in the business of selling computing resources in the form of Virtual Private Server (VPS) and not VPN Services. The Petitioner is not offering dedicated VPN Services like Express VPN etc., but using the OpenVPN and other third party tools which its customers can use to browse anonymously with the purchased seedbox/VPS.

19. Furthermore, it is intriguing that the Petitioner's website contains an article titled "NEED BEST VPN? TOP 5 VPN PROVIDERS". The said article promotes NordVPN, PIA, Express VPN, Cyber Ghost and Proton VPNs. It is interesting to

note that despite the Petitioner claiming to be a VPN Service Provider himself is promoting services of its own competitors. The article is annexed as **ANNEXURE-R3**.

20. Additionally, a perusal of the Petitioner's website shows that it offers "Seedboxes", "Windows RDP", "VPS" and "Root Servers" on rent to general Internet users. It is pertinent to note herein that "Seedboxes" provided by the Petitioner are preloaded with software such as ruTorrent, SickRage, CouchPotato etc., which facilitate users to download movies and shows via torrent as soon as they are released. It appears that said enablement by the Petitioner may contribute in proliferation of online piracy and violation of intellectual property rights. Therefore, identification of the users and retention of logs mandated by impugned directions are essential to safeguard the economic interests and to aid in the analysis of cyber incidents including identification and apprehending of the offenders.

21. It is further submitted that Petitioner has averred that several major VPN service providers such as Express VPN, Surfshark, and NordVPN decided to leave India due to impugned directions, which again depicts that the Petitioner is furthering the cause of those entities before this Hon'ble Court, which they are otherwise not entitled to; and its commitment with our national interest and larger public good of sovereign country is not in sync. The decision of the sovereign countries cannot be allowed to be steered by these multinational companies who have different agenda and goals.

22. Furthermore, the Petitioner's claim that it performs an essential public function of providing VPN services, is nothing but a frivolous one, since the said activity is purely commercial in nature.

NOTARY R.V. SINGH Advocate Regn. No. 2282 GOVT. OF INDIA

III. Impugned Directions do not mandate disclosure of "sensitive personal information"

23. The Impugned Directions do not mandate the Petitioner to register and maintain extremely detailed and invasive personal information of users. In so far all collection and storage of logs as contemplated under Direction (iv) is concerned, the Respondent has amply clarified in the FAQ document, as to what logs are to be stored in ICT systems. The FAQ no. 37 is reproduced below:

> ***"Q 37. What logs need to be stored for ICT systems to help in cyber incident analysis?***
>
> ***Ans.:*** *The logs that should be maintained depend on the sector that the organisation is in, such as Firewall logs, Intrusion Prevention Systems logs, SIEM logs, web / database/ mail / FTP / Proxy server logs, Event logs of critical systems, Application logs, ATM switch logs, SSH logs, VPN logs etc. It may be noted that this list of logs is not exhaustive but has been mentioned to provide flavour of logs to be maintained by the relevant teams. From the incident response and analysis perspective both successful as well as unsuccessful events shall be recorded".*

24. That Respondent has envisaged the requirement of 180 days for maintenance of logs, which has been optimally derived at, on the basis of prevalent practices in the ICT Industry, experience in conducting incident response and analysis of cyber security incidents. The industry best practise is to maintain logs for one year. As part of incident handling, it has been observed that typical cyber-attack by advanced actors spans several months wherein the attack progresses through various stages like reconnaissance/ scanning; weaponization; exploitation ; lateral movement; compromise of critical assets leading to data ex-filtration /sabotage.

25. Therefore, it is evident that stipulation of keeping the logs for 180 days is reasonable and is essential in order to analyse cyber incidents carried out by malicious and nation/ state or non-state actors including those impacting economic, critical infrastructure and national security.

26. Furthermore, the Respondent vide Direction no. (v) has prescribed the collection of data pertaining to basic user data and the rationale of same is with the twin objectives. First, the affected entities or victim of cyber incidents can be reached for suggesting remedial/mitigation measures; Secondly, it will enable information

on identification of the particular subscriber or customer, to remain available with service providers, so that in case of cyber incident or in the matter of contravention of any offence, the said subscriber or customer is duly identified or apprehended as per law of land and create deterrent effect.

27. That provisions of Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 defines the term "sensitive personal data or information", which is reproduced below:

> *" Sensitive personal data or information.— Sensitive personal data or information of a person means such personal information which consists of information relating to;— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) Biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:*
>
> *Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules."*

On a comparison of the information of subscribers/customers sought to be collected as per the impugned directions vis-a-vis the definition of sensitive personal data or information enunciated in abovementioned rules, it is evident that information mandated in the impugned directions are not sensitive personal data or information of any user.

28. Furthermore, the basic subscriber/ customer information directed to be collected and maintained under the impugned directions is to be kept with the VPN/VPS service providers only, like the Petitioner; and the said information is to be shared with the Respondent only when ordered/directed to do so, in relation with cyber incident or cyber security incidents. The same has been clearly enumerated in the direction (iii) of the cyber security directions (reproduced herein below):

> *"When required by order/direction of CERT-In, for the purposes of cyber incident response, protective and preventive actions related to cyber incidents, the service*

NOTARY R.V. SINGH Advocate Regn.No.2282 Commission Expire on 24-10-2027 Area-Delhi GOVT. OF INDIA

provider, intermediary, data centre, body corporate is mandated to take action or provide information or any such assistance to CERT-In, which may contribute towards cyber security mitigation actions and enhanced cyber security situational awareness"

29. Therefore, it is uncontrovertibly evident that Petitioner will be asked to provide information or take action or provide assistance only in given or laid down circumstances in relation to the activities and functions assigned to Respondent, as evinced from a conjoint reading of the Cyber Security Directions. In fact, the same has also been clarified in the FAQ issued by the Respondent:

> ***"Q 20. Do the Cyber Security Directions of 28.04.2022 affect the Right to Privacy of individuals?***
>
> ***Ans.:*** *The right to informational privacy of individuals is not affected by these Cyber Security Directions of 28.04.2022. These directions do not envisage seeking of information by CERT-In from the service providers on continuation basis as a standing arrangement. CERT-In may seek information from service providers in case of cyber security incidents and cyber incidents, on case to case basis, for discharge of its statutory obligations to enhance cyber security in the country. The service providers are bound to protect the users' information by following reasonable security practises and procedures".*

30. It is further submitted that the Hon'ble Supreme Court in the ***Puttaswamy (Supra)*** judgments, has unequivocally observed that the right to privacy is not absolute and is subject to reasonable restrictions. In fact, the Hon'ble Supreme Court has also observed that legitimate state interests ought to be balanced against the individual's right to privacy. Therefore, the impugned directions, which have been issued in furtherance of enhancement of cyber security of the citizens and which only contemplate sharing of a user's data with the Respondent in certain specific circumstances cannot be said to be a violation of an individual's privacy.

31. Furthermore, it is submitted that the Hon'ble Apex Court's decision in ***CPIO v. Subhash Chandra Agarwal (2020) 5 SCC 481*** is not applicable in the present case, as it is based on a completely different set of facts and circumstances; and the said judgment also recognises the test of larger public interest. Further, it is submitted that the cloak of "anonymity" cannot be used to evade from the law.

NOTARY R.V. SINGH Advocate Regn.No.2282 Commission Expire on 24-10-2027 Area-Delhi GOVT. OF INDIA

IV. Under the garb of privacy restrictions, the Petitioner is trying to further its own economic/financial interests

32. The Petitioner on the one hand has claimed that it has provided assistance to law enforcement agencies who have sought specific information about its customers, without any substantiation or probative value terms; and on the other hand has also claimed that Petitioner only collects such personal information as is voluntary provided and it does not maintain logs as it adheres to strict privacy policy and customers use these services to browse the internet almost anonymously. Both the claims of the Petitioner are antithetical and contradictory. If the Petitioner is not having any accurate information about the customer, how will it assist the law enforcement agencies is a moot question.

33. That Petitioner has asserted that it collects such personal information as is voluntary provided in its privacy policy. However, contrary to the impugned assertion of the Petitioner, in the said Privacy Policy itself, the Petitioner has expressed that *" The personal information that you are asked to provide, and the reasons why you are asked to provide it, will be made clear to you at the point we ask you to provide your personal information"*. Further, the Privacy Policy of the Petitioner has envisaged that *"If you contact us directly, we may receive additional information about you such as your name, email address, phone number, the contents of the message and or attachments you may send us, and any other information you may choose to provide"*. The Petitioner has also mentioned therein that *"when you register for an Account, we may ask for your contact information, including items such as name, company name, address, email address and telephone number"*. Therefore, it is evident that the Petitioner does collect basic personal information from its customers contrary to its claim that only non-personal information on voluntary basis is collected by it.

34. Therefore, it is evident that Petitioner is already seeking the somewhat similar information from its customers which is akin to the information of subscribers /customers sought to be collected under the impugned directions.

35. In addition to the above, the Petitioner's privacy policy also provides that the petitioner may use the information so collected by it in the following manner:

"We use the information we collect in various ways, including to:-

- *Provide, operate and maintain our website*
- *Improve, personalize, and expand our website*
- *Understand and analyze how you use our website*
- *Develop new products, services, features, and functionality Communicate with you, either directly or through one of our partners, including for customer service, to provide you with updates and other information relating to the websites, and for marketing and promotional purposes*
- *Send your emails*
- *Find and prevent fraud"*

36. From the above-said usages, it is evident that the Petitioner is observing and also monitoring the activities, as it has expressly stated that it is using information to *"understand and analyse how you use our website"*. The Petitioner claims that *"Petitioner's customer uses these services to browse the internet almost anonymously"*. Here, the term 'almost' is expressed in abstract form without detailing on the observance and monitoring aspects of the activities of customer.

37. In respect of Log files, the Petitioner has disclosed the following practise and procedure in its privacy policy, which is reproduced as under:

"Log Files

SnTHostings follows a standard procedure of using log files. These files log visitors when they visit website of SnTHostings. All hosting companies do this and a part of hosting services' analytics. The information collected by log les include internet protocol(IP) addresses, browser type, Internet Service Provider(ISP), date and time stamp, referring exit pages, and possibly the number of clicks. These are not linked to any information that is personally identifiable. The purpose of the information is for analysing trends, administering the site, tracking users' movement on the website, and gathering demographic information.

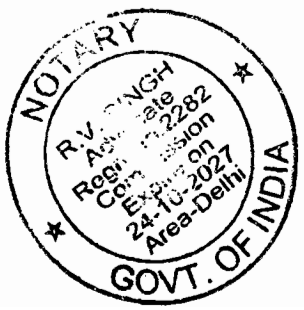
However, we do not maintain any logs of our customers who use any of our services including VPN, VPS, Hosting, or any other services listed on the website. We have a zero-log policy."

38. Therefore, it is clear that the Petitioner is collecting logs and making analysis of trends including tracking users' movement on its website. The user or visitors of Petitioner's website may include customers. Hence, Petitioner itself is engaged in monitoring the activities and gathering demographic information.

39. The Petitioner has also enabled the access of third party advertising Partners as it has disclosed that *"Third party ad servers or ad networks uses technologies like cookies, JavaScript, or Web Beacons that are used in their respective advertisements and links that appear on SnTHostings, which are sent directly to users' browser. They automatically receive your IP address when this occurs. These technologies are used to measure the effectiveness of their advertising campaigns and/or to personalize the advertising content that you see on websites that you visit. Note that SnTHostings has no access to or control over these cookies that are used by third party advertisers"*. Further, the Petitioner has also disclosed that *"SnTHostings's Privacy Policy does not apply to other advertisers or websites"*.

40. Furthermore, it is submitted that although the Petitioner is an Indian entity and catering to customers in the territory of India but its privacy policy, it has stated to be amenable to the California Consumer Privacy Act (CCPA) rights and General Data Protection Regulations (GDPR) Data protection rights, but there is no mention or willingness of the Petitioner exhibited in the Privacy Policy of the Petitioner, about the compliance with the IT Act and the Rules thereunder.

41. It is further submitted that the Petitioner, is, in fact an "intermediary", defined under Section 2(w) of the IT Act, since is providing network services and engaged in transmitting the electronic records on behalf of user.



[(w) "intermediary", with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes;]

42. Therefore, in view of the rule 3(1)(j) and (l) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, the Petitioner is, in fact bound to provide information to any government agency, sought in relation to any cyber security incidents.

> *"3 (1) (j) the intermediary shall, as soon as possible, but not later than seventy two hours of the receipt of an order, provide information under its control or possession, or assistance to the Government agency which is lawfully authorised for investigative or protective or cyber security activities, for the purposes of verification of identity, or for the prevention, detection, investigation, or prosecution, of offences under any law for the time being in force, or for cyber security incidents: Provided that any such order shall be in writing stating clearly the purpose of seeking information or assistance, as the case may be;*
>
> *(l) the intermediary shall report cyber security incidents and share related information with the Indian Computer Emergency Response Team in accordance with the policies and procedures as mentioned in the Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013."*

43. It is further submitted that the Respondent has been engaged with the concerned stakeholder even after the issuance of impugned directions and even extended the timelines for MSMEs for about 90 days and Petitioner has also claimed to be a MSME but has exhibited its unwillingness in compliance with these directions. Although, the Petitioner has challenged the impugned directions, but has not complied with direction no. (iii) also, as even by 30.11.2022, the Petitioner has not informed the Respondent about the designated Point of Contact for interfacing with Respondent. Whereas these directions become effective on 25.09.2022 for MSMEs , which, inter-alia, provides the following:

> *'The service providers, intermediaries, data centres, body corporate and Government organisations shall designate a Point of Contact to interface with CERT-In. The Information relating to a Point of Contact shall be sent to CERT-In in the format specified at Annexure II and shall be updated from time to time. All communications from CERT-In seeking information and providing directions for compliance shall be sent to the said Point of Contact."*

44. It is submitted that the Petitioner has filed the present Petition due to financial constraints brought out as one of ground stating that the storage of data, as

mandated by the impugned directions would require some resources. However, said financial constraints cannot be a ground for challenging the impugned directions.

45. It is further submitted that the Hon'ble Apex Court in ***R.K. Garg v. Union of India and Others (1981) 4 SCC 675*** has clearly enumerated that a legislation pertaining to economic matters is empiric and based on experimentation; and even though there may be crudities, inequities and even possibilities of abuse of the same, however, the same cannot be a ground enough to strike it down as invalid.

PARA-WISE REPLY:

1. The contents of Paras 1-26 of the Writ Petition are denied for the reasons mentioned herein above in the preliminary submissions as well as the reply on merits, unless specifically admitted therein.

2. The contents of Para 27 of the Writ Petition are denied.

3. The contents of Para 28 of the Writ Petition are denied for want of knowledge.

4. The Respondent reserves the right to file an additional affidavit, in the interest of justice, and in order to assist this Hon'ble Court for the purposes adjudication of the present writ petition.

PRAYER

Therefore, in light of the above-mentioned facts and circumstances, the Respondent most humbly prays that this Hon'ble Court may be issued to:

a. Dismiss the present writ petition with costs; and/or

b. Any other order(s) or relief(s) as this Hon'ble Court may deem fit and proper in the facts and circumstances of the present case.

NOTARY R.I. SINGH Advocate Regn. No. 45342 Commission Expiry on 24-10-2027 Area-Delhi GOVT. OF INDIA

VERIFICATION

Verified at Delhi on this 8 DEC 2022 day of December, 2022 that the contents of the above affidavit are true to my knowledge ~~on the basis of~~ documents derived from records and nothing material has been concealed therefrom.

DEPONENT

CERT-IN
Min. of Ele. & Inf. Technology, MD-3

[redacted]