CERT-In New Directives for VPN: A Growing Focus on Mass Surveillance and Data Privacy

Neeraj Jayant, Naman Nanda, Sushila Madan, and Anamika Gupta

Abstract Digitalization efforts are rewarding as Information Technology is bringing changes in almost every sector. Virtual Private Network (VPN) was expected to be a safeguard for sensitive and personal information for individuals. The focus of India's cybersecurity watchdog, Indian Computer Emergency Response Team (CERT-In), focuses on safeguarding or prevention with feasible effort. It is difficult to maintain data privacy without hampering user identity. CERT-In directives try to enhance cybersecurity by bridging the gap in cyberincidence analysis. VPN is ever growing with Bring Your Own Device (BYOD), Work From Home (WFH) in place. A VPN allows users to browse the Internet while masking their device's IP address, encrypting data, and routing through secure networks in other states or countries with no logs. The new CERT-In directives emphasize obligatory data collection, retention, and integration for Virtual Private Server (VPS) providers, VPN services, and Cloud providers for a minimum of 5 years. There is an urgent need to increase the security of the country's digital infrastructure in the best feasible ways, but some new directives may not be privacy-friendly hampering user identity and data protection framework. It has major market implications and an increase in operational costs. Thus, making an Un-CERT-In time for VPN providers in India. This directive does not only defeat the purpose of VPNs but is also possibly aimed at state-sponsored surveillance. We have proposed a few solutions to go through this new rule for the end users.

Keywords CERT-In directives · Data privacy · Information security · VPN · Surveillance · OpenVPN · Data protection framework

N. Jayant (✉) · N. Nanda · S. Madan · A. Gupta
Delhi University, New Delhi 110089, India
e-mail: neeraj21713@sscbs.du.ac.in

N. Nanda
e-mail: naman21712@sscbs.du.ac.in

A. Gupta
e-mail: anamikargupta@sscbsdu.ac.in

© The Author(s), under exclusive license to Springer Nature Singapore Pte Ltd. 2024

S. J. Patel et al. (eds.), *Information Security, Privacy and Digital Forensics*,
Lecture Notes in Electrical Engineering 1075,
https://doi.org/10.1007/978-981-99-5091-1_7

1 Introduction

CERT-In aims at strengthening the country's cybersecurity infrastructure and is taking adequate steps for the same. The new directives that were released by CERT-In on April 28, 2022 aim at logging of the user data and presenting it to the government as and when required. The services that need to adhere to this directive are the cloud service providers, data centers, and VPN companies. The directives come out to be the complete opposite of what these service providers claim to provide, that is, "anonymity" [1]. There are two sides to the coin one being the cybersecurity concerns pertaining to the country and the second being the breach of privacy and mass surveillance by the government. We aim to emphasize and pinpoint the important aspects of the directives and provide a viable solution for the same.

VPN is developing exceptionally quickly. The impact of recent innovations and COVID-19 has led to major changes in the industry with Bring Your Own Device (BYOD) and Work From Home (WFH) increasing the need for security [2]. VPN was expected to be a safeguard for sensitive and personal information for the individuals. Our examination demonstrated that almost 50% of users use VPNs for general security reasons, such as staying away from identity theft. While 40 percent involved VPNs for general protection from hackers and their snooping on public networks [3]. The other 10% used it for more uncommon reasons which were bypassing school, office, school, or government restrictions set by firewalls [4]. VPN provides a sense of security as it ensures the traffic is encrypted and passes through a secure tunnel preventing any leaks. Thus making it a preferred choice over proxy servers. India is one of the countries with the most noteworthy VPN use. This might be somewhat in light of the fact that there isn't a lot of web opportunity in India [5]; occupants have limited admittance to virtual entertainment and "negative substance" which can incorporate the accompanying pornography, psychological oppression, extortion, hate speech, misleading data, defamation, etc.

- The other major use cases of VPN are as follows:
- Data privacy from your ISP.
- Data privacy from the Government.
- Safety on a public Wi-Fi.
- Blocking malware when accessing the Internet.
- Secure access to networks when accessed remotely.
- Access to geolocation-specific content.

A user installs a VPN client which helps them encrypt the data that is being sent over to the VPN server using VPN protocols. The ISP is unable to identify the encrypted data and simply forwards the requests to the VPN server. The VPN server does the rest by hiding the IP and geolocation of the user. The user is able to surf the Internet anonymously while connected to the VPN (Fig. 1).

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) together create a VPN connection where the host is a web browser and the user has restricted access to the application. Online shopping portals commonly use these protocols. Web

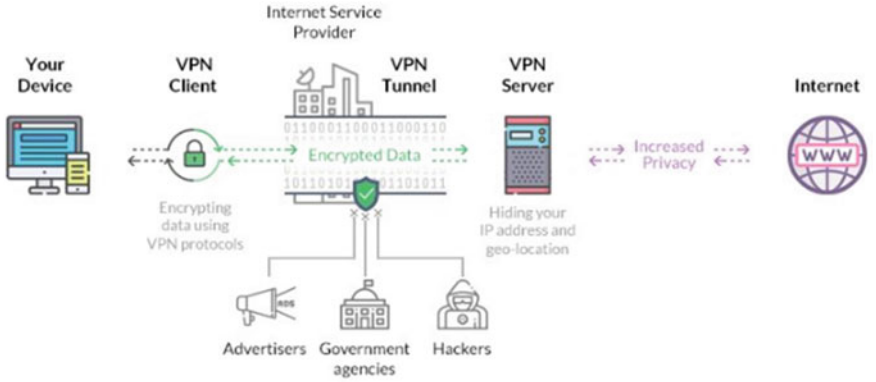

Fig. 1 A figure caption is always placed below the illustration. Short captions are centered, while long ones are justified. The macro-button chooses the correct format automatically [6]

browsers can easily switch to SSL as they are embedded with both SSL and TLS. "HTTPS" in the first part of the URL denotes a SSL connection instead of "HTTP". The ISP, however, sees the following information when you use a VPN:

- The IP address of the VPN server.
- The timestamp of when you connected.
- The port your VPN protocol is using.
- The amount of data you're sending or receiving.
- Encrypted and unreadable data traveling between you and the VPN server.

1.1 VPN Protocols

PPTP—The point-to-point tunneling protocol developed by Microsoft is one of the oldest protocols in existence [7]. The protocol was essentially used for dial-up connections.

L2TP/IPSec—PPTP was replaced by the Layer 2 Tunneling Protocol. The protocol itself is not very secure and needs to be used in unison with a security protocol. It is usually clubbed with the IPSec protocol [8].

SSTP—Secure Socket Tunneling Protocol is a very popular protocol that has been used by Microsoft ever since Windows Vista was introduced [9]. This protocol is popular because of the 2048 SSL/TLS for encryption and 256-bit SSL keys.

OpenVPN—This is an open-source protocol with the strongest encryption. Being open source, the underlying code of the protocol can be accessed and modified according to the requirements of the developer [10]. This protocol is more popular because of its open source and strong encryption capabilities.

There have been a lot of research papers on the technical aspects of VPN, the security they use, and the technologies that they use for encryption or data transmission.

A case study based on a real-world scenario has never been published or discussed. There are works based on GDPR and its impacts on privacy and advertisement-providing companies (Tobias Urban, Dennis Tatang, Martin Degeling; June 2020) [11]. Our research focuses mainly on the average Indian user and the repercussions of the new directives by the governing body. The ways to deal with the scenario change that will be brought forth with it. We aim to emphasize and pinpoint the important aspects of the directives and provide a viable solution to manage the data privacy from CERT-In new directives and VPN mass surveillance, impacting the Indian companies.

2 Discussion

2.1 New CERT-In Guidelines and Its Repercussions

The Indian Computer Emergency Response Team (CERT-In) released a new privacy rule in April 2022 asking all the VPN companies, cloud companies, and data centers functioning in India to hold customer data and Information and Communication Technology (ICT) transactions for a period of 5 years. They released this in an effort to counter cyberattacks and strengthen the online security of the country. The new guidelines would require VPN administrations and other cloud specialist co-ops to log all client information and ICT exchanges over a period of time. The VPN business has reproved the new mandates, saying that such tough regulations conflict with the essential reason and strategy of Virtual Private Networks. Some of the top VPN providers have already eliminated their actual Indian servers.

The detailed analysis of the rule mentioned in Directive 5 is that the Data Centers, VPS providers, Cloud Service providers, and VPN companies need to hold the user's information for 5 years or longer and hand it over to the government as and when required by them. The data should be held even after the user has canceled their subscription [12]. This meant that any VPN company residing in India with physical servers need to store the following information:

- Full name and address.
- Phone number.
- Email address.
- Actual IP address.
- New IP address (issued by the VPN).
- Timestamp of registration.
- Ownership pattern of customers.
- Purpose of using the VPN.

The study demonstrates a correlation between the many VPN-providing companies that have already pulled off their business from India by taking down physical servers [13]. They will however continue to operate in India by providing virtual

servers. A virtual server is a software representation of a physical server. It surely provides the functionality of a physical server but also lacks the underlying machinery and power. The issues with virtual servers are that they are very high resource hogging and perform low. A physical server that hosts many virtual servers creates this issue and users face the issues of lower bandwidth and slower load times [14]. Thus, the biggest advantage of virtual servers is that they can redirect the data and don't force the user to abide by the new Section 70B directives for VPS services. Moreover, these guidelines also issue a statement regarding the cloud service providers and crypto- or virtual asset-providing companies. According to the directives, virtual asset exchange providers and custodian wallet providers as defined by the Ministry of Finance from time to time shall mandatorily maintain all Know Your Customer (KYC) details [12] and records of financial transactions for a period of 5 years. These again hint toward the breach of the identity of an individual.

According to reports, India is pushing for international action to stop unauthorized access to technologies like virtual private networks (VPNs), end-to-end encrypted messaging services, and blockchain-based products like cryptocurrencies. Indian officials made recommendations to members of a United Nations Ad Hoc committee that was debating a comprehensive international convention on combating the use of information and communication technologies for criminal purposes saying that "the anonymity, scale, speed, and scope offered to (terrorists) and the increasing possibility that they will remain untraceable to law enforcement agencies" by using these technologies continues to be one of the major challenges the world faces.

This came as a shock to the VPN companies as it is the exact opposite of what they advertise. The VPN companies offer complete anonymity and follow a strict no-log policy. This means that they do not hold or retain any of the customer data. They function on volatile RAM-based servers [15] and as soon as they are powered off the data is lost. The new laws also have created a backlash regarding the privacy of users in India. The Internet Freedom Foundation (IFF) [16] has actively been asking questions regarding the new laws and appealing the annulment of this decision. They claim that the collection of data will prove to be a bigger threat to the cybersecurity of the country and also will result in a breach of privacy of the individuals. It would also mean that the costs of these services will increase as the companies will have more data centers to hold such volumes of data.

Currently, the directives placed in order to curb cybercrime in India are seeking integration challenges to the existing system. There is no law in the country like the General Data Protection Regulation (GDPR). A bill that is pending, known as the PDP bill (personal data protection), is an Indian adaptation of the GDPR of the EU [17]. We have outlined some of the most crucial factors that must be taken into account in the PDP bill in order to address the security implications of the new directives. Once passed as an act, there would be more clarity on the data retention policies and privacy of the user's data held by the VPN, cloud, and data center companies.

2.2 Proposed Solution

This proposed method as per the compliance aspect—The new directives by CERT-In create a lot of ambiguity for the VPN-providing companies as currently there is no law in India governing data privacy and data protection. A bill that is pending, known as the PDP bill 2019 (personal data protection), is an Indian adaptation to the General Data Protection Regulation (GDPR) of the EU. Once passed as an act, there would be more clarity on the data retention policies and privacy of the user's data held by the VPN, cloud, and data center companies.

Currently, the IT Act 2000 is the governing umbrella under which some provisions that safeguard the privacy of the user exist. For example, Section 43 deals with the loss or damage to the personal computer and the compensation that the victim is entitled to by the attacker. Section 43-A [18] specifically deals with the Compensation for Failure to Protect Data. But many organizations or service-providing companies find loopholes and get past them. A PDP bill [19] if enforced will protect the interests of the consumer further and more efficiently. Some of the important aspects of the PDP bill are mentioned below:

1. Right to Access Data Handling—This gives the individuals a right to request information about their data from the data fiduciary. They can also request to ask if their data has been processed by the data fiduciary or not. Organizations engaged in profiling or observing the behavior of Indian citizens will be subject to additional requirements. The individuals can request a summary of how their data has been processed. The data fiduciary needs to submit the information to the individual in a clear and readable format.
2. Right to Control Personal Data—The individuals have a right to correct misleading or inaccurate personal data. They have the right to complete/update the incomplete personal data. They also have the right to erase personal data that is no longer required by the data fiduciary for the purpose for which it was processed. Organizations must adopt security procedures that enable them to keep track of information and activity and safeguard information by creating contracts in writing with vendors.
3. Right to Data portability—The individuals have the right to obtain their personal data in a structured and machine-readable format from the data fiduciary. This will enable them to transfer, copy, move, and reuse their personal data across different IT environments and services.
4. Right to Data Ownership—Individuals have the right to restrict or prevent the disclosure of their personal data when the data has served the purpose for which it was being collected by the data fiduciary.
5. Right to Data Breach Notification: Data breaches must be reported by organizations to the appropriate authorities and, in some cases, the impacted individuals.

The PDP bill is based on the guidelines of the GDPR of the EU and is directed toward the data privacy and protection of individuals. Once this bill is passed as an

Fig. 2 GDPR and data logs

act there would be less ambiguity and confusion related to any of the new directives that may be released by CERT-In in the future pertaining to data and its privacy and protection.

This other proposed method of creating and implementing most secured, open-source, and self-reliant VPN—currently, VPN companies are not bound to audits as there are no trails left behind. After these laws come into action, there would be ease of auditing and the service-providing companies would be kept in check (Fig. 2).

If the PDP bill is not passed by the government and things continue to function as they are, the users could create a self-hosted VPN [20] and continue surfing the Internet without the interference of the new directives. Self-hosted VPNs are nothing but a user creating a VPN of his own by purchasing a VPS of his choice. Self-hosted VPNs are simply VPNs that a user creates on his own by selecting and paying for a VPS. Users with an IP from that particular country are able to browse the Internet owing to the VPS of that nation. Data is encrypted over a tunnel while the user's original IP address is hidden, ensuring their anonymity. Numerous websites offer the option for customers to buy a VPS and browse incognito. These virtual private servers are governed by local laws in that area. This is due to the fact that the physical servers needed to route user traffic are situated there. CERT-recommendations In's advise keeping logs on people who use the services.

The whole purpose of this solution is to have a secure and reliable VPN connection to be able to access the Internet. The new laws according to CERT-In would not be applicable to self-hosted VPNs. The main emphasis is on security and which is why we would be using the most secure protocol currently available which is OpenVPN. This protocol being virtually unbreakable and open source can be modified according to the requirements and also makes use of SSL/TLS tunneling making it highly

secure in setting up a connection. It uses AES-256-bit encryption and 2048-bit RSA authentication and a 160-bit SHA1 [21] hashing algorithm.

The users can set up a VPS using Linux, purchase a VPS, and use the OpenVPN protocol as the underlying mechanism for creating a VPN. The users can then connect to the Internet using this VPN connection to safeguard their data. We will also add another layer of security which would be Time-Based One Time Password (TOTP) for authentication [22]. This would assure that the users are authenticated well before using the VPN services (Fig. 3).

If the users wish to connect to the Internet to access specific geolocated services or content, they can purchase a VPS (multiple available online) and set up a VPN to access that content.

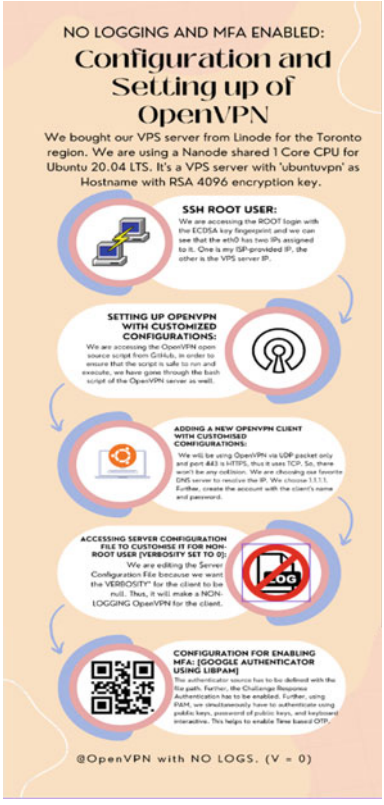

Fig. 3 Flowchart for configuring customized VPN

3 Conclusion

There are many operational and market implications that hinder the idea of implementing new directives laid down by CERT-In. Reporting within 6 hours will impair the efficiency of flow management [23]. An adequately structured laid-down risk-based approach should be followed to improve the approach to collection and management of data logs for VPS, VPN, and cloud providers keeping the operational costs and risk appetite of the business in regard. Therefore, achieving a cyber-secured nation is a constant effort, it is essential to being a positive game plan by balancing cybersecurity with the right to privacy, market implications, and security concerns. The proposed solution aims to alter the PDP bill with GDPR directives that give the right to the end user that can be edited/deleted/stored/manipulated [24]. The alternate approach is to configure a VPS to set up your own VPN server that can be configured with no data logs, data privacy, and multi-factor authentication.

4 Future Aspects

The reporting of cyberincidents from the security perspective is complex, and the new directives are vague in terms of data privacy stated by IFF (Internet Freedom Foundation). The new rules are exempted from central agencies and rigorous clauses around storing data logs within the permitted area of the country could lead to some major VPN and cloud providers diverting advantageous future investments in India. On August 3, 2022, the center withdrew the Personal Data Protection Bill 2019 after the Joint Committee of Parliament recommended 81 changes in the proposed law. A clearer picture of the Personal Data Protection (PDP) bill is required considering the Personal Identifiable Information (PII) [25] and Protected Health Information (PHI) for ease in portability, and other important information. For laying down an important bill like this, the cyberwatchdog, CERT-In, should refer to the industry standards and requirements for stating important rules and regulations for data processing.

References

1. Vyas R (2022) New VPN rules and how it alters your privacy. https://economictimes.indiatimes.com/tech/technology/ettech-explainer-what-indias-new-vpn-rules-mean-for-your-privacy/
2. Ferguson P, Hutson G (1998) Everything about VPN. Research paper revised in Cisco systems
3. Vojinovic I (2022) VPN Statistics for 2022—"keeping your browsing habits private" https://dataprot.net/statistics/vpn-statistics/
4. Anand A (2022) The increasing rate of cybercrime in India. https://www.cnbctv18.com/india/cyber-crime-are-on-a-rise-in-india-amit-shah-cyber-security-ncrb-data-13913912.htm
5. Shim T (2022) The many use-cases of VPN: how a VPN can be useful https://www.webhostingsecretrevealed.net/blog/security/how-a-vpn-can-be-useful/

6. Tim Mocan (2018) How does a VPN server work. https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-a-vpn-server-how-does-a-vpn-server-work/
7. Harry S (2020) All about PPTP, via GeeksForGeeks https://www.geeksforgeeks.org/pptp-full-form/
8. Vojinovic I (2022) What Is the L2TP VPN Protocol?": An outdated protocol we still use out of convenience. https://dataprot.net/guides/what-is-l2tp/
9. Dahan M (2021) How to use a VPN with secure socket tunneling protocol (SSTP). https://www.comparitech.com/blog/vpn-privacy/vpn-sstp/
10. Josh (2020) What is OpenVPN? how it works & when to use It in 2022. https://www.allthingssecured.com/vpn/faq/what-is-openvpn/
11. Urban T, Tatang D, Degeling M, Holz T (2019) Study on subject data access in online advertising after GDPR. International workshop on data privacy management, luxembourg
12. Ministry of Electronics and Information Technology (MeitY), Government of India (2022) CERT-In_Directions_70B. https://cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf
13. Sharwood S (2022) ExpressVPN moves servers out of India to escape customer data retention law. https://www.theregister.com/2022/06/02/expressvpnservers_out_of_india/
14. Max S (2021) VPN server location: physical servers vs digital servers. https://www.cloudwards.net/virtual-server-vs-physical-server/
15. Vishwanath A (2021) The laws for surveillance in India, and concerns over privacy. https://indianexpress.com/article/explained/project-pegasus-the-laws-for-surveillance-in-india-and-the-concerns-over-privacy-7417714/
16. Internet Freedom Federation (2022) CERT-in directives are vague https://twitter.com/internetfreedom/status/1521797466496004097
17. Sen P (2021) EU GDPR and Indian data protection bill: a comparative study. Indian Institute of Technology (IIT), Kharagpur. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3834112
18. Pal Dalmia V (2011) Data protection laws In India. https://www.mondaq.com/india/it-and-internet/133160/data-protection-laws-in-india#:~:text=Under%20Section%2043A%20of%20the,any%20person%2C%20then%20such%20body
19. Veera Vanamali K (2022) Why does India doesn't have the PDP bill yet. https://www.business-standard.com/podcast/economy-policy/why-does-india-not-have-a-data-protection-bill-yet-122080500071_1.html
20. Perkins S (2022) Self Hosted VPNs. https://www.androidpolice.com/how-to-make-personal-vpn-30-minutes/
21. OpenVPN community (2022) OpenVPN cryptographic layer. https://openvpn.net/community-resources/openvpn-cryptographic-layer/
22. OpenVPN community (2022) TOTP multi factor authentication. https://openvpn.net/vpn-server-resources/google-authenticator-multi-factor-authentication
23. Thathoo C (2022) Cyber security incidents within 6 hours To CERT-In. https://inc42.com/buzz/report-cyber-security-incidents-within-6-hours-to-cert-in-govt/#:~:text=%E2%80%9CAny%20service%20provider%2C%20intermediary%2C,%2C%E2%80%9D%20CERT%2DIn%20said
24. Baig A (2108) What GDPR has for the VPN users. https://www.globalsign.com/en/blog/what-gdpr-means-for-vpn-providers-and-users
25. Burchfiel A (2022) India's personal data protection bill impact businesses. https://www.tokenex.com/blog/ab-how-will-indias-personal-data-protection-bill-impact-businesses