Internet Impact Brief

India CERT-In Cybersecurity Directions 2022

Neeti Biyani, Andrei Robachevsky, Internet Society
Prateek Waghre, Internet Freedom Foundation
Contributors: Carl Gahnberg, Joseph Lorenzo Hall, Karen O'Donoghue, Olaf Kolkman, Rajnesh D. Singh, Internet Society

1 June 2022

Abstract

The new cybersecurity directions from the Indian Computer Emergency Response Team (CERT-In) lay out a new cybersecurity framework for service providers, intermediaries, body corporate, data centres, and government bodies against various threats and breaches. It seeks to address gaps and loopholes in the cybersecurity regulations in the country.

This report uses the Internet Impact Assessment Toolkit (IIAT) to assess how the draft regulation may affect Internet development in India, and more broadly, the health of the global Internet. It finds that CERT-In's directions, specifically the overbroad mandate for all entities to synchronize their time with the government's servers and for them to maintain all their ICT system logs for a period of 180 days, could have serious repercussions on the usefulness of the Internet for India and its people. The CERT-In directions endanger the very sectors that the regulation seeks to foster and protect. If enacted in its current form, the regulation could curtail the country's digital transformation without imparting clear benefits for its economy and society.

To ensure that India and users in the country continue to benefit from the Internet and its contributions to the burgeoning national tech sector, the cybersecurity directions' provisions must align with those that make the Internet an open, globally connected, secure, and trustworthy resource for all.

Methodology

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). This includes: an accessible infrastructure with a common protocol, a layered architecture of interoperable building blocks, decentralized management and distributed routing, a common global identifier system, and a technology-neutral, general-purpose network. To assess whether the present proposal has an impact on the Internet, this report will examine its impact on the IWN foundation the Internet needs to exist, and what it needs to thrive as an open, globally connected, secure and trustworthy resource.

Context

On 28 April 2022, the Indian Computer Emergency Response Team (CERT-In) issued new cybersecurity directions under section 70B of the parent legislation, the Information Technology Act, 2000 (IT Act). CERT-In is the government-appointed nodal agency tasked with performing cybersecurity-related functions. The directions relate to information security practices, procedure, prevention, response, and reporting of cybersecurity incidents. CERT-In further released a set of frequently asked questions on the new directions in May 2022. The directions are expected to come into effect at the end of June 2022, 60 days after their announcement.

CERT-In announced these new directions in an attempt to address serious problems that India has had lately with cyber crime and compromise of data. India has witnessed an alarming number of cybersecurity related incidents—the number stands at 1.4 million incidents in 2021 and 212,000 incidents in January and February 2022 alone. While a number of big data breaches occurred within large companies including Domino's, Unacademy, and Air India, India's government authorities reported 48,285 cybersecurity incidents in 2021, most notably from the government's Covid19 database, and the Common Admission Test database.

According to an IBM survey conducted in 2021, the average cost of a data breach in India is ₹165 million (roughly US$2.12 million). The average mean time to identify a data breach stood at 239 days, and the time to contain a data breach at 81 days.

A direct result of these breaches and incidents is that Indian users' personal data is available to third parties over the Internet for nefarious use. Most of these incidents are not flagged by entities that own and control this data (i.e. data fiduciaries), but instead by independent cybersecurity researchers. According to CERT-In, there are regulatory gaps in handling cybersecurity incidents and interactions, which have been hindering incident analysis and their ability to help staunch the flood of breached data. The cybersecurity directions were proposed to address these gaps.

The directions apply to the following entities offering services in India:

- **Service providers,** such as telecom service providers, network service providers, internet service providers, web-hosting service providers, cloud service providers, and cryptocurrency exchanges and wallets
- **Intermediaries,** such as social media platforms, search engines, and e-commerce platforms
- **Body corporate**, which include any company, firm or proprietorship
- **Data centres,** which store and process large quantities of private and public data
- **Government bodies**

The directions lay out the following requirements:

- Cybersecurity incidents need to be reported within six hours: All entities are required to report any cyber incidents to CERT-In within six hours of noticing the event, in contrast to the existing rules, which expect entities to report incidents "as early as possible".
- Synchronization of clocks: All entities covered under the new directions must connect to the Indian government's clocks including the Network Time Protocol (NTP) server of the National Informatics Centre (NIC), the National Physical Laboratory (NPL), or to servers traceable to these NTP servers for synchronization of all information and communication technology (ICT). However, not all entities are required to comply with this requirement—entities with ICT infrastructure spanning multiple countries, such as cloud service providers, can use accurate and standard time sources other than NPL and NIC, as long as there is no deviation from these government designated clocks.
- Maintain ICT systems logs for 180 days in India: All entities in the scope of the directions must enable logs of all their ICT systems and maintain the same for 180 days within the Indian jurisdiction. CERT-In reserves the right to order that it is provided with these logs in the light of any cybersecurity incident.
- Cryptocurrency exchanges and wallets must maintain know-your-customer (KYC) details and financial transaction records for five years: Virtual asset service providers, virtual asset exchange providers, and custodian wallet providers now need to maintain information regarding customers engaged in cryptocurrency transactions through KYC, as well as financial transaction records for five years. CERT-In says that this requirement needs to enable reconstruction of "relevant parties including IP addresses along with timestamps and time zones, transaction ID, the public keys (or equivalent identifiers), addresses or accounts involved (or equivalent identifiers), the nature and date of the transaction, and the amount transferred".
- Service providers must maintain customers' and subscribers' information for five years: Data centres, virtual private server (VPS) providers, cloud service providers, and virtual private network (VPN) providers are required to register and maintain the names of customers and subscribers, period of hire, IP addresses allotted to or used by customers, email address and IP address and time stamp at the time of registration, purpose of hiring such services, validated address and contact numbers, and the ownership patterns of subscribers for a period of five years, even after the cancellation or withdrawal of such subscription.
- CERT-In can order action and demand information: The new directions give CERT-In the power to issue orders to entities mandating them to take action or provide information that assists CERT-In to prevent, pre-empt or address cyber incidents. Such orders could also include the format in which the information is required, the timeframe which could include up to and including near real-time, and the timeframe within which such information must be provided to CERT-In. Entities not adhering to these requirements risk being tagged as non-compliant and facing punitive actions that can include imprisonment for a term of up to one year or a fine of up to 100,000 rupees, or both under Section 70B(7) of the Information Technology Act, 2000.

- **Designate a point of contact to interface with CERT-In**: Similar to the 2021 Indian IT Rules, entities must appoint a point of contact to interact with CERT-In. CERT-In will in turn seek information and provide compliance guidelines to the designated point of contact.

However, several provisions of these directions threaten the experience of an open, globally connected, secure, and trustworthy Internet in India, with significant extraterritorial effects, and go against global industry best practices with regard to cybersecurity procedures. The absence of a data protection law in the country further exacerbates the effects that the directions will have.

How do CERT-In's Cybersecurity Directions Affect the Internet?

In order to understand how the CERT-In directions could affect the Internet itself we assess how it might impact the Critical Properties of the Internet as described by the Internet Society:

Decentralized Management and a Single Distributed Routing System

One of the fundamental properties of the Internet is that it is a network of networks— over 73,000 independent networks[1] choose to collaborate with one another and connect with each other voluntarily. Each network makes decisions regarding its own operations and security, based on its needs and local requirements. There is no central direction, or a controller dictating how and where connections are made, so the network grows organically, driven by local interests and needs. This results in several crucial benefits that make the Internet so successful—global reach, resilience and optimized connectivity. This property also allows a 'permissionless' model of networking that the Internet is built upon, and allows users and innovators to make use of this agility, scalability and adaptability offered by the Internet.

Many entities deploy their own time servers which are engineered to meet the resiliency and accuracy requirements of their networks and services. These services are often synchronized to global time standards. To require all entities to synchronise all their ICT systems clocks to the Indian government's Network Time Protocol (NTP) Server of the National Informatics Centre (NIC), or to the National Physical Laboratory (NPL), or to servers traceable to these NTP servers goes against the critical properties of the Internet. Such a requirement creates a real risk of a single point of failure and vulnerability, and goes against industry best practices for synchronizing to multiple sources of time.

[1] In the context of routing, there are more than 73,000 Autonomous Systems operating on the Internet. An Autonomous System is a group of networks with a single routing policy defining how the network connects and exchanges traffic. The networks in an Autonomous System are usually under a single operational and administrative control.

Additionally, there are more than 3,000 publicly available NTP servers on the Internet at present. Industry best practice encourages connecting to multiple NTP servers simultaneously. This enables the NTP algorithms to determine which is the best overall source of time. Risks such as noise in measurements, network delays, and network asymmetries are mitigated by connecting to many NTP servers, as long as the servers are reasonably independent of each other. This independence of varied sources of time helps to ensure resilience against all sorts of errors and even time-based attacks on systems themselves. Companies have also highlighted concerns that synchronization with NIC and NPL NTP servers or to servers traceable to these NTP servers could "negatively affect companies' security operations as well as the functionality of their systems, networks, and applications", as there is uncertainty about their capacity and inadequacies surrounding latency issues.

The CERT-In directions negatively impact the decentralized nature of network management and operation by requiring all entities and servers to connect to the NTP servers at the NIC or NPL. In the case of companies with infrastructure spanning multiple geographies such as cloud service providers, they are required to use their own time source as long as it does not deviate from NPL and NIC time. Forcing all entities and service providers to comply with this direction would create large chokepoints, putting each of them at risk of impact by failure.

Mandating such centralized technical compliance requirements leads to monocultures, and compromises the agility needed to solve problems that may occur in networks such as issues with routing or time infrastructure. While coordinating a response is important in case of cyber incidents, collaboration between affected entities—each doing their own analysis and taking agreed actions—is the most effective response.

Furthermore, the directions take a 'one size fits all' approach to the requirement of maintaining logs. Mandating all entities to retain all of their ICT logs for a period of 180 days is an extremely broad approach, creating a honeypot of log information. Instead of specifying what logs are necessary, such as security logs, and what entities are essential and important for India based on a proper risk assessment, the directions cover everything. This will be a significant hurdle for small and medium enterprises (SMEs) who might not have the financial resources or have the capacity to maintain such enormous archives of their logs. This could have the unintended consequence of suppressing innovation and allowing only large tech companies to be able to operate in India.

How do CERT-In's Cybersecurity Directions Affect the Realization of the Full Potential of the Internet?

The critical properties are what is needed to have the Internet, but they are not sufficient if we want the Internet to reach its full potential. To assess how this proposal might impact what we need for an Internet that is open, globally connected, secure, and trustworthy, this analysis will look at it through the lens of what enables these goals.

Easy and Unrestricted Access

It is easy to become part of the Internet, for networks and users alike. That means that for users the Internet is affordable and Internet services are accessible, and that networks can easily become part of the Internet, without unnecessary regulatory or commercial barriers for both groups.

The Internet was built and developed in a voluntary, decentralized and permissionless manner. This 'permissionless' model that the Internet is predicated upon presents lowest possible technical barriers to new actors when they choose to enter, connect to or innovate on the Internet. This implies that there are no unnecessary barriers presented to connecting to and building services on top of the Internet's infrastructure. The CERT-In directions counter this principle by requiring all service providers, intermediaries, data centres, body corporate, and government organisations to mandatorily enable logs of all their ICT systems and maintain the same for a rolling period of 180 days. In doing so, the CERT-in directions discourage new actors from easily entering the market by significantly raising the barriers for entry, and pose considerable challenges for existing entities.

Logging is generally considered a good practice, but there are vast differences in the types of logs generated and the information they contain. While keeping information about security-related events that happen on a system is important, many other types of logs may not hold information of similar or greater value and do not require such careful treatment. Not all entities are the same—some play an essential role in providing services for the digital infrastructure in India when compared to others. The 'one size fits all' approach undertaken by the directions will result in significantly higher costs of doing business in India, and increase the burden of compliance, thus making the Internet less accessible for new users and actors. It is more important than ever for networks and services to be secure and agile to be able to respond to cybersecurity challenges. It is therefore essential that CERT-In implements a focused approach based on risk assessment and industry best practices.

The directions impose conditions on no-log VPNs and other zero-knowledge systems to retain information that was not being logged to begin with. This opens up questions about the continued legality of such services as they operate currently, and risks cutting off users in India from accessing them.

Roughly 60 crore (0.6 billion) Indians still cannot access the Internet, and the aim is to connect them all in the next few years. The country also aspires to fulfill its objective of achieving a $1 trillion digital economy by 2026. SMEs have a key role to play in helping this national ambition, and will increasingly rely on the digital infrastructure available to them to engage in trade and service delivery. The CERT-In directions will create barriers for SMEs to easily connect to the Internet or rely upon it for their purpose.

Collaborative Development, Management, and Governance

The Internet's technologies and standards are developed, managed, and governed in an open and collaborative way. This open collaboration extends to the building and operation of the Internet and services built on top of the Internet.

The top-down approach to the CERT-In directions contradict the principle of collaboration that is fundamental to how the Internet works and best practices in cyber security. The development of the Internet has always been based on voluntary cooperation and collaboration, underpinned by collective responsibility. This is the core of the collaborative security approach, with multi-stakeholder cross-border collaboration at its heart. The Internet, being a network of networks, is an interconnected, interdependent system. No one participant on the Internet can achieve absolute security, and no security solution exists in isolation.

Cyber incidents, similar to disasters and crises, are best addressed collaboratively, where the multi-stakeholder model is adopted and various entities are involved. Creating security and trust in the Internet requires different players (within their different responsibilities and roles) to take action, closest to where the issues are occurring. Most often, for greater effectiveness and efficiency, solutions should be defined and implemented by the smallest, lowest or least centralized competent community at the point in the system where they can have the most impact. Such communities are frequently spontaneously formed in a bottom-up, self-organizing fashion around specific issues (e.g. spam, or routing security) or a locality (e.g. protection of critical national infrastructure, or security of an Internet exchange).

This is a more effective way of addressing cybersecurity incidents than a top-down, prescriptive approach represented in the new directions.

Data Confidentiality of Information, Devices, and Applications

Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating.

Data confidentiality is highly dependent on correct time. The CERT-In directions put data confidentiality at risk by undermining time security. This issue is further examined in the next section.

Integrity of Information, Applications, and Services

The integrity of data sent over the Internet, and stored in applications, is not compromised. That is, information sent over the Internet shouldn't be modified in transit, unless directed by the communicating parties (e.g., a captioning bot may be useful to turn spoken words into text).

A lot of security services rely on precise and accurate time, and making sure time is reliable is an important goal. However, the rules as currently written undermine the resiliency of Indian users. One of the main purposes of the NTP protocol is that it eradicates clocks with the wrong time by comparing several sources of time. Ideally an NTP instance takes its time from at least three sources that do not share a common source. If CERT-In provides a high quality stable NTP service to Indian users, CERT-In will be able to improve the diversity and thereby the reliability of the time system. By forcing all users in India to use clocks that depend on one source they completely undermine the resiliency offered by using diverse sources of time.

To promote time security and network resiliency, CERT-In should operate independent high precision NTP servers based on stable reference clocks and advertise (instead of mandate) the best practice of using multiple NTP time sources of which the CERT-In clock is one. If the CERT-In clock is stable and well-reachable the NTP protocol will converge to use it, without any mandate. Another important requirement that is missing from the CERT-In time recommendation is that NTP servers should support Network Time Security (NTS)—a standard that is designed to ensure that the time network is getting is coming from a trusted source and is not modified by an attacker.

Reliability, Resilience, and Availability

The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable.

As highlighted above, CERT-In's directions pose significant risks to reliability. It requires all entities and servers to connect to the Indian government's NTP servers of the National Informatics Centre or the National Physical Laboratory, or to servers traceable to these NTP servers for synchronisation of all their ICT systems clocks. This creates a significant risk of a single point of failure and vulnerability.

There are also uncertainties about the location, geographical distribution, and configuration of the NIC and NPL servers. In a system where everything is dependent on the time drift not being more than a nanosecond, it is important that any questions about the configuration, latency, service levels, and time sources of the NIC and NPL servers be clearly and publicly answered. There are also concerns about the capacity of the Indian government's servers, and whether the NIC and NPL servers are able to serve potentially millions of entities and billions of devices hitting the same set of servers from the perspectives of technical capacity, budget, and human resources.

Accountability

Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way.

Across the world, Computer Emergency Response Teams (CERTs)—also known as Computer Security Incident Response Teams (CSIRTs)—are commonly established to coordinate communications among security and computer experts during emergencies and to help prevent future computer security incidents from occurring. The role of all CERTs is fairly comparable—all of these organizations are dedicated to responding to cybersecurity incidents to regain control and minimize damage, to providing or assisting with effective incident response and recovery, and to preventing computer security incidents from re-occurring.

Generally, the primary mission of CERTs is to act as a trustworthy partner of the public and private sectors in responding to and resolving cybersecurity incidents. It is noteworthy that the foundational values underpinning the establishment of CERTs were the same as those of the Internet—voluntary collaboration and trust.

The new directions transform CERT-In's mandate, undermining the collaborative and voluntary nature of its primary mission. The requirement to report a broad range of incidents within six hours risks overwhelming CERT-In with large volumes of reports, compromising its ability to undertake any 'emergency response'.

CERT-In also oversteps its mandate in asking virtual asset service providers, virtual asset exchange providers and custodian wallet providers—cryptocurrency exchanges and wallets—to maintain information for five years about their customers and transactions through the Know Your Customer (KYC) norms. This should not be part of the CERT-In directions. Instead these services and service providers should be regulated through financial statutes, compliance mechanisms, norms and practices.

The directions expand the remit of CERT-In and make it less effective. They also threaten to incapacitate CERT-In, as network operators and service providers will be reluctant to acknowledge and share details of incidents if CERT-In is also acting in a law enforcement or regulatory role. Since CERTs are a critical component of collaborative security, clouding CERT-In's mission will also undermine the Internet's security.

Privacy

Privacy on the Internet is the ability of individuals and groups to be able to understand and control what information about them is being collected, and to control how this is used and shared. Privacy often includes anonymity.

Increasing amounts of personal data are being digitized for various purposes such as public service delivery, e-commerce, trade, employment, education, communication, recreation, and so on. Each user's digital footprint is expansive, and users rely on strong privacy tools such as encryption and data privacy laws to keep their information safe online.

The overbroad and blanket requirement on all service providers, intermediaries and entities to collect and retain all their ICT logs for a period of 180 days, as mandated by the CERT-In directions, creates significant vulnerability and privacy risks. Without specific categories of logs that specific entities need to maintain, all entities and organizations maintaining all their logs for 180 days goes against the universally accepted principle of data minimization, which is central to maintaining privacy. Said differently, data that is not collected or that is securely disposed of cannot be breached. It is unfortunate that one of the most effective technical mechanisms we have to protect against data breach—data minimization and destruction—is exactly what CERT-In is forbidding with the new directions, effectively requiring massive data retention.

The directions are not aimed at individual users, but they adversely impact individual agency by eliminating their consent from the equation. By forcing zero-knowledge services to log information they even disregard and negate a user's choice to use such services to begin with. It is also unclear how these directions will interact with the Right to be Forgotten / Erasure as applicable in India now, or in the future.

Further, the ambiguous requirement on part of entities to furnish information to CERT-In when directed to do so does not indicate how this information will be used, nor provide sufficient safeguards that it will not be used in other contexts or for different purposes. The potential for penal provisions that may include imprisonment skews incentives towards overcompliance. This creates the risk of information retained under these directions being used for surveillance.

CERT-In also mandates data centres, VPS providers, cloud service providers, and VPN providers to engage in the collection of data that they simply do not need to, such as contact details including addresses and phone numbers, purpose of hiring such a service, and ownership patterns—and especially if a user discontinues their use of these services. Further, the requirement to collect and store IP addresses alloted / being used are ambiguous in the context of VPN services. It is unclear why this type of information is needed, and how it will be used.

Services such as VPS and VPN providers, which by design do not collect data, should not have to collect data that are not relevant to their operations to satisfy the new directions, just as private spaces cannot be mandated to carry out surveillance to aid law enforcement purposes. It further creates a situation where data that could not be breached before now must be collected and protected against breaches and rogue uses of such data.

Zero-knowledge systems enable security and anonymity over the Internet, discourage tracking and profiling and help keep users safe on the Internet, especially vulnerable and marginalized sections of society. CERT-In's directions risk diluting the essence of these tools that keep all of us safe when we are online.

The directions violate the Right to Privacy recognised under Article 21 of the Indian Constution. They are also not in line with the principles of proportionality and lack procedural guarantees as enshrined in the Puttaswamy test.

What makes CERT-In's directions related to data collection even more risky is that India does not have a data privacy law nor a data protection law. Therefore, citizens in the country do not have the surety that their data will be safeguarded against overuse, abuse, profiling, or surveillance.

The current draft of the data protection bill provides sweeping exceptions to the state. Thus, the existence of requirements to retain logs that may include personally identifiable information, coupled with the lack of procedural safeguards, will have a chilling effect on speech.

Summary and Conclusions

This analysis, based on the Internet Impact Assessment Toolkit, has found that several provisions contained within the new CERT-In directions present concerns and adverse repercussions for the open, globally connected, secure and trustworthy Internet.

The directions introduce significant compliance costs and burdens, especially for small and medium enterprises in the country, and for new actors looking to enter the burgeoning tech industry, thus making the Internet *less open* for those who want to use it.

Its overbroad mandate for all entities to connect to government-mandated NTP servers and log all ICT systems logs, as well as its prescriptive model of addressing cyber incidents, do not align with the fundamental principles of collaborative security, thus *limiting global connectivity.*

A lack of specificity around which entities and logs are essential to India's cybersecurity, and the requirement to centralize valuable personal and business data, essentially make personal and business data more vulnerable to malicious actors, resulting in a *less secure* Internet for Indian users. The extraterritorial impact of the directions on service providers and intermediaries also risk India's leadership in the ICT sector, and the growth of its digital economy.

The directions do not define the configuration and capacity of the government's servers, and do not define the scope of use of information demanded from entities. Coupled with the lack of a data protection law in the country, the directions risk making the Internet and online services in India *less trustworthy* and appealing for users, effectively hindering the growth of the tech industry in the country and the Digital India vision.

To better align the CERT-In directions to global norms and best practices, the following considerations must be taken into account:

- CERT-In should reconsider the 'one size fits all approach', and take into account the decentralized nature of network management, where depending on multiple servers for accurate time is a long-established practice. The mandate for all entities to connect to the National Informatics Centre or the National Physical Laboratory NTP servers, or to servers traceable to these NTP servers for synchronization of all ICT systems, risks creating large chokepoints where failure would impact all Indian entities and service providers. There are also significant concerns about the configuration and capacity of NIC and NPL NTP servers. Integrity and reliability of the time is essential for many security services, including encryption, electronic signatures, DNSSEC, and routing security, and achieving these objectives is critical.
- Because security of networks and services and the requirement to effectively respond to cybersecurity challenges have never been higher, it is essential that CERT-In implements a focused approach based on risk management and industry best practices. CERT-In should conduct a comprehensive risk assessment, and specify the categories of entities and logs such organizations must maintain. An indiscriminate approach which expects *all* entities to maintain *all* ICT systems logs creates high compliance costs and burdens, limits the ability of SMEs to operate well, hinders new actors from entering the Indian tech sector, and creates a honeypot log of information which will be easy for malicious actors to target. The lack of a data protection law creates further ambiguity for the use or abuse of such data.
- The requirement for entities to report cyber incidents within six hours of noticing them is not aligned with global best practices. The EU's General Data Protection Regulation (GDPR) allows a three-day window to report breaches. There are multiple other concerns resulting from this requirement, such as entities, especially SMEs, unable to hire staff around the clock to comply with this requirement. CERT-In must identify the most important vulnerabilities, severities, and criticalities that need to comply with the six-hour timeline, allowing second- and third-level criticalities more time to report cyber incidents.
- CERT-In was essentially established to coordinate communications among security and computer experts during emergencies and to help prevent future computer security incidents. It should therefore not deviate from its original mandate. By requiring broad access to logging information, CERT-In takes responsibilities typical for a law enforcement agency, which is not its role or part of its mission. In asking cryptocurrency exchanges and wallets to collect and provide the information mentioned in the new directions, CERT-In is essentially stepping into the role of being a financial watchdog. This will require specialist expertise and resources, and will likely result in it being unable to properly fulfil its role.
- CERT-In should also clearly lay out the scope of use of information demanded from entities in case of cyber incidents. This is crucial for privacy of users' and business data, given that the country does not have a data protection law at present.