1 June, 2022

International coalition of organisations and individuals calls on CERT-in to strengthen privacy and cybersecurity by withdrawing the Directions issued on April 28, 2022.

To,
Shri Sanjay Behl
Director General
Indian Computer Emergency Response Team (CERT-in)
Ministry of Electronics and Information Technology
Government of India
Email: info@cert-in.org.in

CC
Shri Alkesh Kumar Sharma
Secretary
Ministry of Electronics and Information Technology
Government of India

Sir,

We write to you to express our concerns with respect to the Directions issued by the Indian Computer Emergency Response Team (CERT-In) on April 28, 2022, under Section 70B of the Information Technology Act, 2000 ("Directions"). The undersigned individuals and organisations share a commitment to strong cybersecurity standards, privacy, freedom of expression, and encryption. We respectfully urge you to withdraw the Directions, as they would weaken cybersecurity, amplify the risk of surveillance, particularly for journalists and human rights defenders, and jeopardise the right to privacy in India.

Below are some of our key concerns with the Directions:

Imposition of data retention requirements that weaken privacy and cybersecurity: Individual privacy for each of us is a prerequisite for strong cybersecurity for all of us. The Directions mandate that (a) service providers, intermediaries, data centres, body corporate and Government organisations maintain logs of all ICT systems for 180 days; and (b) data centres, virtual private server providers, cloud service providers and virtual private network service providers (VPNs) register customers' information, including names, emails and IP addresses, ownership patterns and purpose for hiring services, for 5 years or more. These data retention requirements put people's privacy at risk. They expand the scope of mass surveillance, contravene globally recognised principles of necessity and proportionality, and data minimisation, and ultimately weaken cybersecurity. They effectively create new cybersecurity vulnerabilities in the form of databases of retained data that can be exploited by malicious actors. Further, many service providers, including VPNs, follow privacy-respecting practices and do not collect any users' data. Such services are crucial for people to exercise the right to privacy

protected by the Indian Constitution and international human rights law. The Directions would compel such service providers to fundamentally alter their services or exit the Indian market, to the severe detriment of people's rights. This is particularly problematic given the absence of a data protection law in the country.

Onerous and incomplete reporting requirements: CERT-In's intention to strengthen cybersecurity incident reporting requirements is appreciated. However, the 6-hour period within which service providers are required to report cyber incidents to CERT-in are too onerous, and contrary to global best practices, which allow for at least 72 hours. Further, the requirement to report cyber incidents within 6 hours from noticing them will require companies to ensure staff presence 24x7, which is infeasible for small and medium enterprises. Infeasible reporting requirements will lead to inefficiencies, and failure to achieve transparency and accountability. Further, an essential component of effective reporting of cyber incidents is timely and comprehensive notification to users and affected parties, which the Directions fail to provide for. Finally, reporting mechanisms have limited value if there is no accountability on the follow-up actions and investigations that would be undertaken by authorities, including CERT-in in this case, to mitigate damage, enable transparency and protect data.

Implicit data localisation mandate and surveillance risks: By requiring entities to maintain logs of all ICT systems for 180 days "within the Indian jurisdiction", the Directions impose burdensome data localisation requirements. This would facilitate increased surveillance, particularly in the absence of any safeguards, given the lack of progress on data protection legislation and surveillance reform. It would also hamper cross border data flows, and impose onerous cost and compliance burdens, serving as discentives, particularly for small and medium enterprises and foreign companies.

Lack of clarity on application; and uniform treatment of dissimilar service providers: The Directions contain ambiguous and overbroad terms which will lead to lack of clarity in respect of implementation. For instance, it is not clear which entities are covered by the terms "body corporates", "service providers", "government organisations" and others. The Directions run the risk of effectively covering all entities linked to the internet, and subjecting them to identical compliance terms, without any tailoring for different platforms. For instance, providers linked with critical infrastructure may be made to comply with a higher threshold of accountability, but the Directions fail to identify such distinctions (potentially also clashing with the directions of the National Critical Information Infrastructure Protection Centre). Further, the types of cybersecurity incidents listed in Annexure I should be unambiguously defined – for instance, the difference between "data leak" and "data breach", what would be construed as a "fake mobile app" and "suspicious activities" should be clarified to enable effective implementation.

Connection to NTP servers that raises security and surveillance concerns: Requiring all service providers, intermediaries, data centres, body corporates and government organisations to connect to the Network Time Protocol (NTP) Server for synchronisation of all ICT systems clocks will increase the attack surface of adversaries and result in insecurity, increased surveillance and inefficiencies.

Synchronisation would create a single point of failure, susceptible to attack. Further, it would expose the location and other details of all servers, which is problematic from a surveillance standpoint.

Absence of consultation: The Directions were formulated without open consultation to take into account feedback from all stakeholders - including the public, civil society, cybersecurity experts, privacy advocates and the private sector. This is also made clear by the FAQs on the Directions, which state that the Directions were framed based on consultations with industry and government organisations from time to time, pointing to the selective, unstructured and informal nature of interactions. A process of in-depth consultation, with the full range of stakeholders, is integral to the development of a framework that meaningfully strengthens cybersecurity and privacy.

Therefore, to protect privacy and cybersecurity in India and on our global internet, we urge CERT-in to withdraw the Directions, and initiate a process of in-depth and sustained multi-stakeholder consultation to inform the development of any directions aimed at strengthening cybersecurity; and the central focus of any such effort should be to enhance privacy, without which robust cybersecurity cannot be achieved.

1 June, 2022

ORGANIZATIONS

Access Now
Africa Media and Information Technology Initiative (AfriMITI)
Article 19
Association for Progressive Communications (APC)
Charles Donaldson Ogura
Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
Committee to Protect Journalists
Internet Freedom Foundation
Internet Society
Kapil Goyal
Laboratory of Public Policy and Internet (LAPIN)
Ranking Digital Rights
Software Freedom Law Center (India)
Tech for Good Asia
Youth Forum for Social Justice

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For More Information, please contact:
Raman Jit Singh Chima | Asia Pacific Policy Director and Senior International Counsel | raman@accessnow.org