INTERNET POLICY NEWS DIGEST | 15-31, JANUARY 2020 | ISSUE 35 www.icrier.org

NEWS DIGEST

MEITY Chair on Internet Policy

ICRIER's Internet Policy News Digest is your update on Indian and global developments in cyber-security, digital economy, and Internet governance. We have recently re-designed the news digest to include opinion pieces covering issues both global as well as focused on India. We sincerely welcome your valuable feedback and comments at www.internetpolicy.in. Please email your valuable feedback and comments to internet.news@icrier.res.in.

GLOBAL

There is a lot of uncertainty regarding the regulation as well as the accuracy of the facial recognition technology the world over. However, Bruce Schneier writing for the New York Times explains how banning facial recognition technology may eventually be a futile exercise in today's day and age. While facial recognition poses serious threat to privacy, other technological devices also have the wherewithal to violate individual autonomy. In this regard, an article in the Conversation discusses the privacy concerns raised by devices such as Amazon Echo and the Alexa and how their interaction with other services may increase the risk of creating a surveillance State. Shoshana Zuboff, the author of "The Age of Surveillance Capitalism" explains how surveillance capitalism has grown unabated over the past two decades in a largely unregulated fashion. Writing for the Harvard Business Review, Bhaskar Chakravorti discusses at length on why 'users' may find it difficult to exercise agency over their own data and why legislative fixes or initiatives undertaken by Big Tech corporations may be a more plausible solution.

European Union is considering a five years ban on facial recognition

The European Commission has revealed it is considering a ban on the use of facial recognition in public areas for up to five years. The regulators require time to come up with a robust methodology for assessing the impact of this technology and possible risk management measures, which may be identified and developed. The proposed ban allows exceptions for security projects as well as research and development. Furthermore, the Commission has proposed imposing obligations on both developers and users of artificial intelligence, and urged EU countries to create an authority to monitor the new rules.

Chinese court rules AI-written article is protected by copyright.

A court in Shenzhen, China, has ruled that an article generated by artificial intelligence (AI) is protected by copyright. Tencent, a Chinese company has been publishing content created by Dreamwriter, an automated software over the past five years. In 2018, an online platform operated by a company called Shanghai Yingxun Technology Company replicated an AI-generated financial report from Tencent on its own website. Even though, the article included a disclaimer that said it was “automatically written by Tencent Robot Dreamwriter”, the court found that the article’s articulation and expression had a “certain originality” and met the legal requirements to be recognised as a written work as a consequence of which it qualified for copyright protection.

Clearview AI might end privacy and lead to a dystopian future

Clearview AI helps law enforcement agencies match photos of unknown people to their online images scraped from Facebook, YouTube, Venmo and numerous other websites. The company has devised a facial recognition app, which allows you to take a picture of a person, upload it and thereafter see public photos of that person along with links to where those photos appeared. With approximately 3 billion images, the system thus far appears to be the largest such database. The US Federal and state law enforcement officers have admitted to using the app to solve shoplifting, identity theft, credit card fraud, murder and child sexual exploitation cases. Facial recognition technology has always been controversial and Clearview’s app exacerbates privacy risks because law enforcement agencies are uploading sensitive photos to the servers of a company whose ability to protect its data is untested.

AI needs to be regulated: Alphabet CEO Sundar Pichai

At the World Economic Forum in Davos, the CEOs of the big tech giants came together to discuss the future of Artificial Intelligence. Alphabet and Google CEO Sundar Pichai acknowledge the need to for new regulations for Artificial Intelligence (AI). He further stated that companies such as Google cannot build new technology and let market forces decide how it will be used. It is equally incumbent on tech companies to ensure that technology is harnessed for good and is available to everyone.

Microsoft admits data breach of 250 million records

Microsoft has acknowledged a data breach of 250 million Microsoft users due to “misconfiguration of an internal customer support database”, which the company uses for tracking support cases. This includes logs of conversations between Microsoft support agents and customers of 14 years. While a large portion of the leaked data like “emails, contact numbers, and payment information” were redacted, a significant part of the leaked data reportedly was also in plain text, which included, but was not limited to, customer email addresses, IP addresses, locations, Microsoft support agent emails, case numbers, resolutions, and remarks and internal notes marked as “confidential”.

More than 30 million debit, credit card records put online for sale

In one of the biggest card breaches reported until now, credit and debit card data of more than 30 million cardholders was leaked and put online for sale, according to a report by a cyber-intelligence company Gemini Advisory. In addition to American cardholders, the breach also advertised the credit and debit card details of over 1 million foreign cardholders on the dark web. In the report, Wawa an east coast based convenience store and gas-station chain has been identified as the source of the breach.

US issues cybersecurity warnings over flawed medical devices

The US has issued warnings after cybersecurity flaws were detected in medical monitoring devices manufactured by GE Healthcare Systems (GEHC). Safety notices were published by both the US Food and Drug Administration (FDA) and the US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) regarding vulnerabilities in certain clinical information central stations and telemetry servers.

The FDA said the vulnerabilities "may allow an attacker to remotely take control of the medical device and to silence alarms, generate false alarms and interfere with alarms of patient monitors connected to these devices."

.

INDIA

The vast amount of data that the increasingly digital Indian population is providing makes Indian consumers highly susceptible to cybercrime. Tushar Verma discusses how the proposed legislation falls short of safeguard a person's fundamental right to privacy as articulated in the Puttaswamy case, particularly the exemption that permits the government to access personal information to maintain the "sovereignty and integrity of India". In contrast, this piece explains how the government's Personal Data Protection Bill is a step in the right direction since it mandates "explicit consumer consent" for data usage and provides the consumer with the authority to delete their information from company databases, thus enhancing consumer privacy.

Meanwhile, writing for the livemint Rahul Matthan makes a strong case for an international treaty on the use of the internet. He argues that lack of internationally agreed principles regarding the use of internet leads to conflict between local interests and international corporations.

Niti Aayog to develop National Data and Analytics Platform

Niti Aayog is preparing to release the National Data and Analytics Platform (NDAP) in 2021 with the objective of "modernising" the think tank's data system and to make government data accessible to stakeholders in a user-friendly manner. The NDAP will seek to improve the accessibility of government data to all users by hosting multiple datasets and presenting them in a user-friendly manner along with different visualisation and analytics tools.

Bahrain and Karnataka sign MoU for cooperation in technology

In accordance with the long-standing economic relations between Bahrain and India, a Memorandum of Understanding (MoU) was signed between The Bahrain Economic Development Board and Government of Karnataka to promote cooperation in Artificial Intelligence, FinTech and other emerging technologies. The agreement was signed at the World Economic Forum's 50th annual meeting at Davos.

Airport's facial recognition data will be deleted

India's DigiYatra initiative, which sought to facilitate paperless travel through facial recognition technology at airports eases the entry of passengers at airports through automatic facial recognition, has raised privacy concerns among travelers. Addressing these concerns, aviation minister Jayant Sinha has stated that the system is compliant with the norms laid under the General Data Protection Regulation (GDPR) and all the information pertaining to the traveler is deleted upon the completion of the trip.

Technology think tanks suggest measures to improve cybersecurity

Technology policy think tanks and digital freedom advocates have written to the National Security Council Secretariat urging stronger encryption requirements, improved breach disclosure norms and use of open-source software while encouraging free flow of data across borders, as part of suggestions to strengthen cyber security in India. These recommendations were submitted as a response to the government's invitation for inputs to a new cybersecurity strategy, which the Indian government plans to release this year. The overarching goal of this policy would be to tackle challenges including data privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime and cyber terrorism.

Malware attacks witness a drop from 2018 to 2019

According to Kaspersky Security Network reports, India observed a “moderate” decrease in cybercrimes during 2019 as compared to 2018. As such, 38.8 per cent of the overall Indian Kaspersky users were attacked at least once by a web-based attacks in 2019 as compared to 2018 when it was 40.4 per cent. These threats include file-less malwares, social engineering attacks and other attacks that were targeted through the world wide web. However, riskware attacks increased from 28 per cent in 2018 to 39 percent in 2019.

Firms split on sharing data with government

In a survey of 5000 companies, 45% of the organisations were against sharing the anonymous data that they generated through their operations with the government, while 45% of the organisations were in agreement with the provisions requiring sharing of data and 10% of the organisations were unsure about the proposition. Such sharing, according to the organisations against the provision, should only be permitted if necessitated by a law-order investigation or enforcement situation. On the other hand, some startups are of the view that sharing of data in the absence of explicit customer consent would violate terms and conditions with their existing customers.

India plans to mandate cyber security measures for power grids

As per the draft rules published by the Central Electricity Regulatory Commission, Indian electricity grid operators will be required to install firewalls and other such measures used by companies to avert an attack on their information technology systems and check rising hacking incidents of power networks across the world. Furthermore, grid operators and regulatory agencies will need to have a continuity plan handy in the event of a cyber-attack.

We’d love for you to spread the word! Do share contact details of those who may be interested in receiving ICRIER’s newsletter, publications and notices regarding seminars, workshops, conferences, etc.

Rajat Kathuria
Director & CE

Core 6A, 4th Floor, India Habitat Centre, Lodhi Road, New Delhi-110003
PH: +91 11 43112400, E-mail: ahuja@icrier.res.in
Website: www.icrier.org

Disclaimer:
Opinions and recommendations in the report are exclusively of the author(s) and not of any other individual or institution including ICRIER. This report has been prepared in good faith on the basis of information available at the date of publication. All interactions and transactions with industry sponsors and their representatives have been transparent and conducted in an open, honest and independent manner as enshrined in ICRIER Memorandum of Association. ICRIER does not accept any corporate funding that comes with a mandated research area which is not in line with ICRIER’s research agenda. The corporate funding of an ICRIER activity does

not, in any way, imply ICRIER's endorsement of the views of the sponsoring organization or its products or policies. ICRIER does not conduct research that is focused on any specific product or service provided by the corporate sponsor.

To unsubscribe please click here