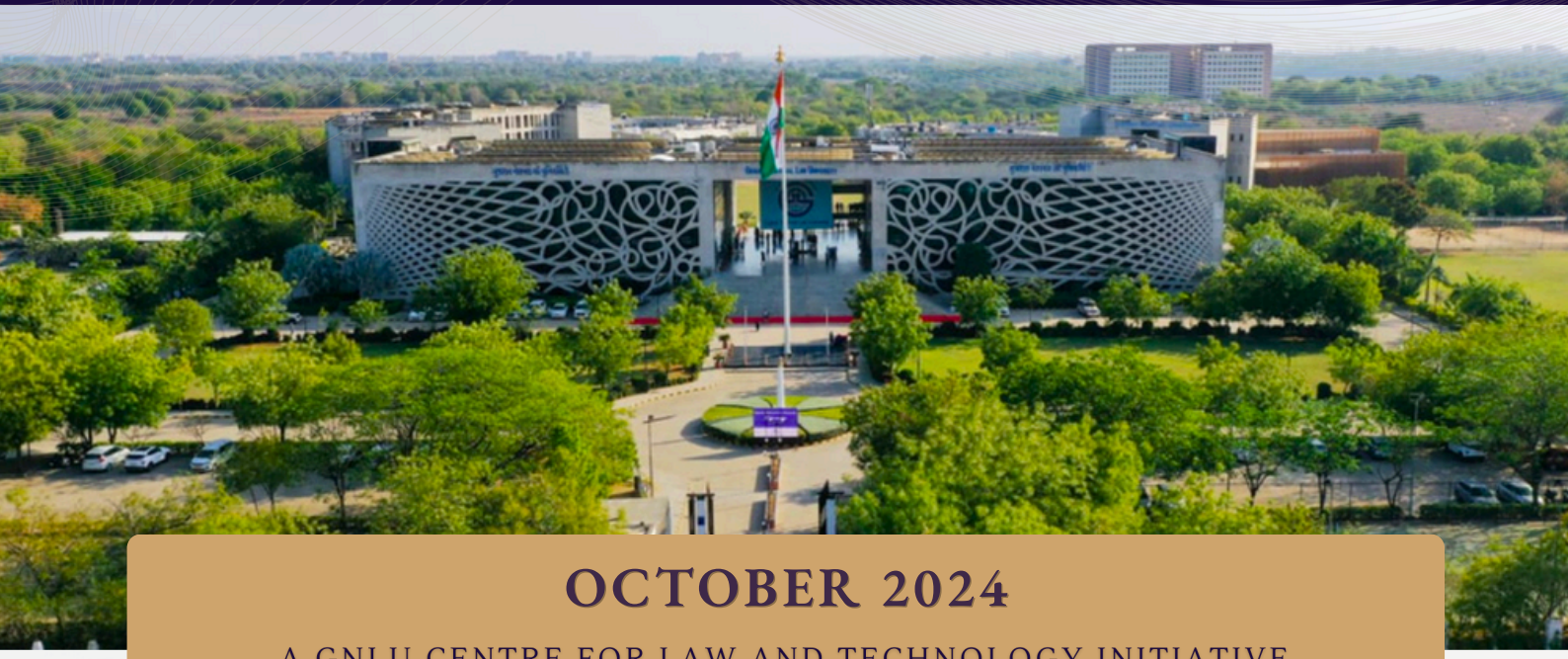
GUJARAT NATIONAL LAW UNIVERSITY
CENTRE FOR LAW AND TECHNOLOGY

VOL 06
ISSUE 10



OCTOBER 2024

A GNLU CENTRE FOR LAW AND TECHNOLOGY INITIATIVE

Monthly Newsletter - TechTalk

Gujarat National Law University

Welcome to the GNLU Centre for Law and Technology Newsletter! Serving as the conduit to the dynamic intersection of science, technology, and the law, our mission is to provide updates on the latest developments, promote academic excellence, and empower legal professionals to navigate this ever-evolving landscape. Join us in bridging the gap between these crucial fields and shaping the future of legal practice in our interconnected world.

Enclosed in this newsletter are the following highlights:

Updates on law and technology, showcasing the latest developments in this ever-evolving field. Our curated content might just spark your next research topic idea. Stay informed and stay inspired and keep reading!

EDITORIAL BOARD (2024-25)

ADVISORS

HEAD OF THE CENTRE

PROF. (DR.) THOMAS MATHEW
PROFESSOR OF SCIENCE AND TECHNOLOGY

CENTRE MEMBERS

PROF. (DR.) ANJANI SINGH TOMAR
PROFESSOR OF LAW

MS. HEENA GOSWAMI
ASSISTANT PROFESSOR OF SCIENCE AND TECHNOLOGY

MS. ANSHU GUPTA
TEACHING AND RESEARCH ASSOCIATE (LAW)

STUDENT CONTRIBUTORS

CHARISSE SUSANNA CH (BATCH 0F 2023-2028)
ARADHANA MINJ (BATCH 0F 2023-2028)
DIPSHIKHA KANJILAL (BATCH 0F 2024-2029)

HEADLINES OF THE MONTH

01 U.S. JUSTICE DEPARTMENT PROPOSES NEW RULES TO PROTECT SENSITIVE DATA FROM FOREIGN ADVERSARIES

The U.S. Justice Department recently proposed new rules to prevent sensitive American data from reaching countries like China, Iran, and Russia. The rules aim to restrict certain business transactions that could expose bulk personal data or federal data, following an executive order from President Joe Biden to safeguard against potential foreign cyberattacks, espionage, and blackmail. In addition to the countries mentioned, the rule extends to Venezuela, Cuba, and North Korea.

This measure reflects Washington's ongoing efforts to curb the flow of American data to foreign adversaries, especially China, amid concerns over trade and technology security. A notable example was the U.S. blocking a 2018 deal for China's Ant Financial to acquire MoneyGram, fearing risks to the privacy of U.S. citizens' data.

The proposal outlines specific types and amounts of data that would be restricted from transfer. For instance, it prohibits the sharing of human genomic data related to over 100 individuals, as well as health or financial data for more than 10,000 people. Additionally, precise geolocation data on over 1,000 U.S. devices cannot be transferred. The new rules would prevent transactions with data brokers who knowingly transfer information to "countries of concern" and restrict data transfers concerning U.S. government personnel.

These regulations empower the Justice Department to enforce compliance through civil and criminal penalties. U.S. officials noted that apps like TikTok could potentially violate these rules if they transferred sensitive data from American users to a Chinese-owned entity. This proposal signifies a step toward limiting foreign access to critical American data, particularly from companies in adversarial nations.

READ MORE

02

UK AND ALLIES SANCTION RUSSIAN CYBER GANG EVIL CORP

The UK imposed sanctions on 16 members of the Russian cybercrime group Evil Corp, alleging that the group has been directed by Russian intelligence to carry out cyber operations against NATO allies. In coordination with the U.S. and Australia, Britain's National Crime Agency (NCA) labeled Evil Corp as one of the world's most significant cybercrime threats. The sanctions aim to signal to Russia that cyber-attacks, whether state-sponsored or from affiliated groups, will not be tolerated, according to Foreign Minister David Lammy.

Evil Corp's leader, Maksim Yakubets, known for his extravagant lifestyle, was indicted by the U.S. in 2019, with a $5 million reward offered for his capture. Yakubets has been linked to Russian intelligence agencies, including the FSB, SVR, and military intelligence GRU. His father-in-law, Eduard Benderskiy, a former FSB official, has been implicated as a key figure in supporting and protecting Evil Corp's activities after the 2019 indictment.

The NCA also revealed Evil Corp's connection to LockBit, a ransomware group involved in high-profile attacks against organizations like Boeing, Britain's Royal Mail, and the Industrial and Commercial Bank of China. Yakubets' associate, Aleksandr Ryzhenkov, has been identified as a LockBit affiliate and has allegedly participated in numerous ransomware attacks. Ryzhenkov was indicted by the U.S. Justice Department for using ransomware, including BitPaymer, to target victims across Texas and the wider United States, stealing data and demanding ransom.

The UK sanctions include asset freezes and travel bans for Yakubets, Artem Viktorovich Yakubets, Viktor Grigoryevich Yakubets, and others. These actions are part of a larger effort by British law enforcement to disrupt two of the most dangerous cybercrime organizations, marking a coordinated international stance against Russian-linked cyber threats

READ MORE

03 BRAZILIAN CONSUMER GROUP SUES SOCIAL MEDIA GIANTS FOR FAILING TO PROTECT MINORS ON SOCIAL MEDIA

Brazil's Collective Defense Institute, a consumer rights group, has filed lawsuits seeking 3 billion reais ($525 million) in damages from the Brazilian units of TikTok, Kwai, and Meta Platforms, alleging that these companies have not implemented sufficient protections to prevent minors from the unregulated use of their platforms. The lawsuits, which highlight growing concerns around social media regulation in Brazil, call for these companies to introduce clear data protection measures and warnings about the mental health risks posed to minors, particularly those under 18, by social media addiction. These demands arise amid increasing scrutiny of social media's impact on young users, spurred in part by a recent dispute between X (formerly Twitter) owner Elon Musk and a Brazilian Supreme Court justice that resulted in significant fines.

Lawyer Lillian Salgado, one of the plaintiffs, emphasized the urgency for platforms to reform their algorithms and data processing practices to provide Brazilian minors with a safer online environment similar to those found in some developed countries. The lawsuits reference various studies indicating that unsupervised use of social media by children and teenagers can harm their mental health and promote addictive behavior.

Meta responded, asserting its dedication to creating safe, age-appropriate experiences for young users and highlighting over a decade of efforts to develop tools and features that support minors and their guardians on platforms like Facebook, Instagram, and WhatsApp. The company also announced plans to introduce a new "Teen Account" on Instagram in Brazil, which will restrict the content visible to minors and control who can contact them. TikTok stated it has not yet received a notice regarding the lawsuit, while Kwai affirmed its commitment to user safety, particularly for younger users. The case reflects Brazil's intensified focus on regulating social media use among minors to protect their mental health and well-being.

READ MORE

04

DELTA SUES CROWDSTRIKE OVER COSTLY GLOBAL OUTAGE CAUSED BY FAULTY CYBERSECURITY UPDATE

Delta Air Lines has filed a lawsuit against cybersecurity firm CrowdStrike in a Georgia state court, seeking over $500 million in damages following a July outage that led to massive flight cancellations, disrupted travel for 1.3 million customers, and affected various industries worldwide. Delta claims the issue originated from a "catastrophic" software update from CrowdStrike that caused 8.5 million Windows-based computers to crash, severely impacting its operations. The lawsuit alleges that CrowdStrike pushed an "untested and faulty" update without proper testing, leading Delta to cancel around 7,000 flights over five days, resulting in significant financial and reputational damage.

CrowdStrike disputed Delta's allegations, calling them "disproven misinformation" and suggesting that Delta's outdated IT infrastructure exacerbated the effects of the outage. The cybersecurity firm admitted a configuration update to its Falcon Sensor software had caused system crashes but questioned why Delta was more affected than other airlines, implying limited liability. Adam Meyers, a senior CrowdStrike executive, expressed regret over the incident before Congress, acknowledging the update's impact and pledging to prevent similar issues in the future.

Delta's lawsuit claims the incident could have been avoided with minimal testing and argues CrowdStrike's actions "crippled" the airline's business by causing delays and significant losses. The U.S. Transportation Department has since launched an investigation into the outage. Delta, which has invested heavily in IT infrastructure, rejects CrowdStrike's claim about outdated systems, asserting its commitment to maintaining advanced technology. Along with the direct costs, Delta seeks compensation for lost profits, legal fees, and reputational harm, contending that CrowdStrike is responsible for the extensive fallout and financial damages caused by the failed update.

READ MORE

05 AMERICAN WATER RESTORES SERVICES AFTER CYBER ATTACK DISRUPTS OPERATIONS

American Water, one of the largest water utilities in the U.S., is addressing a recent cyber attack that led to the shutdown of its systems. Based in Camden, New Jersey, the utility provides drinking water and wastewater services to over 14 million people across 14 states. The breach was discovered on October 3, prompting the company to take immediate action by shutting down its customer portal and pausing billing processes to safeguard its systems.

As of late Thursday, American Water announced that its customer portal, MyWater, is back online and billing has resumed. The company assured customers that there would be no late fees for the period of the disruption and confirmed that water quality was unaffected, with no evidence indicating that its water and wastewater facilities were compromised.

The investigation into the breach is ongoing, and the company is implementing additional security measures to bolster its systems against future incidents. American Water's spokesperson, Ruben Rodriguez, declined to provide further details on the breach or its implications.

American Water has a market capitalization of $26.7 billion and operates over 500 water and wastewater systems in about 1,700 communities, including military installations. Recent reports have raised concerns among U.S. officials regarding potential cyber threats from foreign entities, particularly alleging that Chinese intelligence may be involved in targeting critical infrastructure, such as water treatment facilities.

The incident underscores growing anxieties about cybersecurity in essential services, highlighting the need for enhanced protective measures within the utilities sector.

READ MORE

06 TELEGRAM RESPONDS TO STAR HEALTH DATA LEAK ALLEGATIONS, CLAIMS IT CANNOT ACT AS 'CONTENT POLICE'

In a significant data breach case, India's Star Health and Allied Insurance Company has taken legal action against Telegram and a hacker, alleging unauthorized access and distribution of personal information.

According to reports, a hacker known as "xen Zen" leaked sensitive data, including medical reports of around 30 million Star Health policyholders, through Telegram-based chatbots. Star Health has labeled this incident as "illegal hacking and unauthorized accessing of confidential, sensitive information."

In September, Star Health filed a lawsuit against Telegram and the hacker after a Reuters investigation exposed how Telegram chatbots were leaking this data. A Tamil Nadu court promptly granted a temporary injunction, ordering Telegram to block any chatbots or websites in India that facilitate such data leaks. This order was shared publicly by Star Health in a notice published in *The Hindu* newspaper.

During ongoing court hearings, Telegram's legal counsel responded by stating that while Telegram can take down specific accounts if solid evidence is provided, the platform cannot independently monitor all content due to privacy and feasibility concerns. Telegram insists that it can act only upon concrete proof and not take on a "policing" role.

In response, the Madras High Court has asked Star Health to submit detailed information about the implicated Telegram accounts for possible removal. This case highlights the complex issues of data security, digital privacy, and platform responsibility in India's growing digital ecosystem.

READ MORE

07 MADRAS HC MANDATES CERTIFIED EXPERTS FOR DIGITAL EVIDENCE IN DIVORCE CASES

In a significant ruling, the Madurai Bench of the Madras High Court emphasized the importance of privacy as a fundamental right, including spousal privacy. Justice GR Swaminathan made this observation while hearing a petition filed by a woman challenging a lower court's order that allowed her husband's mobile call records, obtained without her consent, to be used as evidence in a divorce case. The husband had presented the call data to support allegations of adultery.

Justice Swaminathan ruled that evidence obtained by violating an individual's right to privacy is inadmissible. He highlighted that the discretion granted to family courts under Section 14 of the Family Courts Act, 1984, does not justify accepting illegally obtained evidence. The judge also referred to the Law Commission's 94th report, which recommended excluding unlawfully obtained evidence in criminal cases.

The ruling underscores the importance of trust in marital relationships and stresses that violating privacy undermines that trust. The judge also discussed the need for proper certification of electronic evidence.

According to the Information Technology Act, 2000, and BSA, 2023, any electronic evidence presented in court must be accompanied by a certificate from a notified expert. Surprised by the lack of such experts in Tamil Nadu, Justice Swaminathan directed the Ministry of Electronics and Information Technology to notify experts in the state within three months to ensure fair access to justice.

READ MORE

SPOTLIGHTING RESEARCH TOPICS: EMPOWERING RESEARCH PAPER ASPIRATIONS

We understand that embarking on a journey to create impactful research papers can be both exciting and daunting. As you navigate through your academic pursuits, we're here to help illuminate your path and fuel your scholarly ambitions. This section presents a curated selection of broad research paper topics designed to spark your intellectual curiosity and inspire your next paper based on the latest developments of this month. Each topic represents an opportunity for exploration, discovery, and the potential to contribute to the ever-evolving landscape of law and technology. We believe that a well-chosen research topic is the cornerstone of a successful publication, and our aim is to empower you to make informed choices.

- *Data Security and Foreign Espionage*
- *International Cooperation in Cybercrime*
- *Cybersecurity threats from nation-states*
- *Social Media Regulation and Child Protection*
- *Software vulnerability management and vendor liability*
- *Cybersecurity insurance and risk mitigation strategies*

MESSAGE FROM THE NEWSLETTER TEAM

The news articles discussed or included in this newsletter represent the views of the respective news websites. We do not endorse or assume responsibility for the content or opinions expressed in these articles. Our purpose is to bring recent developments to your knowledge, providing a diverse range of information for your consideration. Your input matters to us, and we'd love to hear your thoughts. If you have any suggestions, ideas, or feedback on how we can improve the newsletter or if there's something specific you'd like to see in future editions, please don't hesitate to reach out. Your insights help us grow and ensure we're delivering the content you want.

Stay curious, stay informed!

GNLU CENTRE FOR LAW AND TECHNOLOGY

GUJARAT NATIONAL LAW UNIVERSITY
ATTALIKA AVENUE, KNOWLEDGE CORRIDOR, KOBA,
GANDHINAGAR - 382426 (GUJARAT), INDIA

gclt@gnlu.ac.in | tmathew@gnlu.ac.in

Blog: **GNLU Issues in Science, Law and Ethics**
Journal: **GNLU Journal of Law and Technology**
Website: www.gnlu.ac.in/Centre-for-Law-and-Technology/Home

Explore Past Edition

TechTalk