



APRIL 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!

DATE OF RELEASE: 23.08.2024

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 OF 2023-2028)
HARSH JITENDRA AMIPARA (BATCH OF 2023-2028)
ARADHANA MINJ (BATCH OF 2023-2028)
DIPSHIKHA KANJILAL (BATCH OF 2024-2029)

HEADLINES

USAGE OF INDEPENDENT BROWSERS SURGES AFTER EU'S DMA 03

SC MENTIONED THE ISSUE REGARDING MANDATORY SHARE OF LIVE LOCATION FOR A BAIL. 04

GOOGLE IS TO UNDERTAKE THE ENHANCEMENT OF ITS PRIVACY SETTINGS SO AS TO SETTLE FOR A DATA PRIVACY LAWSUIT 05

CANADIAN BILL TO REGULATE ONLINE CONTENT SPARKED DEBATE OVER FREE SPEECH CONCERNS 06

WORLD-FIRST CYBERSECURITY LAWS FOR SMART DEVICES ENACTED BY UK 07

OPENAI AND MICROSOFT HAVE BEEN ACCUSED OF COPYRIGHT INFRINGEMENT 08

**OF
THE
MONTH**

01

USAGE OF INDEPENDENT BROWSERS SURGES AFTER EU'S DMA

The Digital Markets Act (DMA), an EU regulation, aims to remove the unfair competition that mandated the big tech companies like Microsoft, Apple, and Google to give their users a choice to select web browsers from a “choice screen” rather than defaulting to their own. The CEO of Cyprus-based Aloha Browser, a privacy-focused browser, asserted that from being on the fourth number, EU has now become the second largest market of our company after the spike of users by 250% in EU after the DMA was enacted. Norway's Vivaldi, Germany's Ecosia, and U.S.-based Brave were some of the other independent browsers that noted growth in the number of users. Big companies with immense user bases like U.S.-based DuckDuckGo and Norway-based Opera have also noticed a growth but noted an incomplete choice screen rollout.

Initially, the devices of the tech companies such as Apple and Google were pre-loaded with the companies' default settings, which caused inconvenience to change. After the enactment of DMA, Apple, in addition to Safari, has provided 11 browsers in 27 EU countries, while Google is also gradually enforcing such corresponding options.

Regardless of the growth, smaller browser companies have criticized the new features of the Apple and Google companies, stating them to be slow and cumbersome. Mozilla, the founder of the Firefox browser, observed that only 19% of total iPhone users in the region received the update, which was said to be slower than the previous software updates. CEO of Norway's Vivaldi also stated that the choice screen only appears after clicking Safari, and a list of browsers with no additional information is shown thereafter.

Substantially, when the DMA has caused a stir in the browser market of the EU, the challenges and complications have persuaded the EU to initiate a non-compliance investigation to find out whether Apple is restricting the users to opt for new browser services.

[READ MORE](#)

02

SC MENTIONED THE ISSUE REGARDING MANDATORY SHARE OF LIVE LOCATION FOR A BAIL.

The Hon'ble Supreme Court on 29th April quoted the potential infringement of the right to privacy caused by the mandatory share of the Google Live location of the accused as a condition for granting bail. The said remark was given in a petition that was filed against the order of the Delhi High Court that granted bail to a person of Nigerian national who was accused under the Narcotic Drugs and Psychotropic Substances (NDPS) Act.

The bench, comprising Justices AS Oka and Ujjal Bhuyan, criticized and questioned the efficacy of the condition for granting bail while stating the need for protection of individuals' privacy rights. The bench also noted the potential infringement of an individual's privacy and expressed concerns about the misuse of technology in legal contexts. Though Google, not being a party to the case, asserted that putting such terms for granting the bail isn't effective since it is mere a tool for navigation or identifying the location.

The Delhi High Court in the hearing in May 2022 included the bail conditions to provide their live location to the investigating officer and not to leave the country and appear before the trial court when required. The court, in such conditions, observed the probable violation of the right to privacy under Article 21 of the Indian Constitution. In August 2023, the court ordered the Ministry of Electronics and Information Technology (MeitY) to file an affidavit with elaborated technical aspects of such practice, but they failed to do so, leaving no choice to the court but to seek clarification from Google India. The court then set aside the bail conditions and granted interim bail relief to the accused. A final decision on this matter is anticipated soon, which could significantly include the implications for the use of technology in the judicial process.

[READ MORE](#)

03

GOOGLE IS TO UNDERTAKE THE ENHANCEMENT OF ITS PRIVACY SETTINGS SO AS TO SETTLE FOR A DATA PRIVACY LAWSUIT

Google, in its fourth settlement in four months, agreed to delete billions of data records of millions of Chrome browser users. In the suit of “Chasom Brown et al. v. Google,” the company was alleged of misleading users by keeping a tab on their online activity in Chrome’s incognito mode. To solve this dispute, Google, rather than paying the plaintiff, has agreed to delete the data of users and additionally ensured significant privacy changes. However, the individuals are open to claim damages from the company. Moreover, for the further protection of privacy, the company has agreed to quit using technology that detects when users open private browsers. To enhance users’ privacy, Google will block third-party cookies by default in Incognito mode. Additionally, the disclosures will be updated, which will inform the users about the private browsing data still being collected by the incognito mode.

Google claimed the lawsuit lacked merit and, via a representative, said the plaintiffs had initially demanded \$5 billion but would now get no monetary reward. The company underlined that all that needs to be done is remove outdated technical data that was never associated with a specific person or was brought in for customized purposes.

Prior to this, Google had already spent more than \$1 billion in the settlement of lawsuits that targeted Google’s search engine as well as its advertising business. In the month of December, a suit claiming high fees for app makers was settled by the company. Not long after that, Google was accused of sharing the user’s information through its defunct Google+ platform. And then in March, Google paid a Massachusetts company over the accusation of patent infringement.

[READ MORE](#)

CANADIAN BILL TO REGULATE ONLINE CONTENT SPARKED DEBATE OVER FREE SPEECH CONCERNS

As per the data provided by the National Census Agency, since 2014, an increase in the reports of online sexual offenses against children has been witnessed. In January, tech executives were gathered for a congressional hearing on online child safety. Following which, a bill to address the concern has been proposed by the government of Prime Minister Justin Trudeau. The proposed bill aims for a statutory restriction and removal of harmful material appearing on their platforms, especially that involves children. Moreover, it would create a new regulatory agency with extensive powers like issuing 24-hour takedown orders to companies for child sexual abuse material (CSAM) or intimate media files posted without consent.

Although the bill is widely supported for its potential to address the increasing concerns about harmful online content, the civil and criminal penalties for hate speech in the bill have been criticized. According to critics, some parts of the bill, especially the one addressing the hate speech, will hinder free expression. In Canada, after the bill is enacted, hate will be classified as a separate crime for the first time. However, critics say that it would be erroneous to do so; instead, it can be added as an element to other criminal offenses. The Canadian Civil Liberties Association warned that it would lead to excessive infringement of expressive freedom, privacy, protest rights, and liberty” and would give a new regulatory agency the power to be a “judge, jury, and executioner.” Mr. Trudeau, targeting the penalties and the actions that will be taken against hate speech, was accused of trying to suppress political speech by the right wing and conservative media outlets in the US.

The bill, in addition to regulating various social media sites, will also be applied to pornography and livestreaming websites. However, private message platforms are excluded. The bill also got support from the Meta, which owns Facebook and Instagram. Moreover, the bill has also been backed by the director of the Canadian Centre for Child Protection, Lianna McDonald. She believes that the bill would prevent the unforeseen tragedies or online violence with children that left their parents devastated.

[READ MORE](#)

UK has a history of cyberattacks such as the damaging Mirai attack in 2016, which made the smart products compromise due to weak security features. Subsequently, UK banks, including Lloyds and RBS, were similarly attacked, which caused disruption to customers. In response to these concerns of hacking and cybercrimes, the UK government has enforced a new law, being the first country to do so, that will oblige the internet-connected smart devices to meet minimum security standards in order to improve security protections and protect the consumers from hacking and cyber-attacks.

Key provisions of the law, legally mandates the manufacturers to:

- Safeguard the consumers from the hackers and cyber criminals by preventing them from getting access to the devices, such as smartphones, gaming consoles, and connected fridges, that have internet or network connectivity.
- To ban common and easily guessable passwords like 'admin' or '12345' to prevent vulnerabilities and hacking. In case there is a common password, the user will have to change it during the initial setup.
- To provide information on how to report security issues to facilitate quicker resolutions. Additionally, the manufacturers and retailers will have to be transparent with the consumers about the timeframe to receive important security updates.

Objectives of the act:

- The act will ensure the better security of the consumer's smart devices and also aims to make the UK the global standard for online safety.
- Manufacturers will make the internet-connected products built with security in mind, which will encourage customers to buy them and thus increase the economy.
- By being a part of the government's £2.6 billion National Cyber Strategy, it can enhance the UK's protection and online prominence.
- To ensure that the consumers receive clear information about the product they are buying and make sure they are using it securely.

The new laws are part of the Product Security and Telecommunications Infrastructure (PSTI) regime, which is designed to protect the users of the UK from cyberattacks. Moreover, the Office for Product Safety and Standards (OPSS) can be approached to report non-compliant products.

[READ MORE](#)

OPEN AI AND MICROSOFT HAVE BEEN ACCUSED OF COPYRIGHT INFRINGEMENT

Eight publications, including The New York Daily News, The Chicago Tribune, The Orlando Sentinel, The Sun Sentinel of Florida, The San Jose Mercury News, The Denver Post, The Orange County Register, and The St. Paul Pioneer Press, came together and filed a suit against OpenAI and Microsoft. These newspapers alleged them of copyright infringement over their use of news articles to train their AI chatbots without permission. In the suit, jury trial and compensation were sought, but no monetary damages were demanded.

The publications claim that the companies surfaced the articles behind paywalls without linking them back to the original sources. Thus, reducing the number of subscriptions, affecting the revenue, and depriving the publishers of licensing the content elsewhere. In response, Open AI expressed its unawareness of the Alden's (the parent company of the newspapers) concerns and highlighted its partnership and conversations with other news organizations. On the other hand, Microsoft declined to give any comment. It sought to dismiss the lawsuit with the argument that there had been no actual harm to the newspapers and their claim that the chatbots have replaced the market for news articles is false.

Further, the companies were also accused of misappropriation and trademark dilution. The newspapers stated that the chatbots credited the publications for inaccurate and misleading reporting, damaging the newspapers' reputations and spreading harmful information. The New York Times also mentioned some of the incidents where ChatGPT has provided wrong and misleading information attributing the newspapers, which led it to never being recommended.

This lawsuit has been added to the disputes pertaining to the fight over data used by the power-generative A.I. online information, such as articles, Wikipedia posts, and other data. The lawsuit highlighted ignorance of the policies by many tech companies and transgressing copyright laws to obtain the data to train their chatbots. The newspapers in the lawsuit asserted that the major issue is not merely a business problem for a handful of newspapers or the newspaper industry at large, but it is a critical issue for civic life in America.

[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.

- *Impact of regulatory interventions on market dynamics*
- *Cross-border data transfers and global privacy standards*
- *Global cybersecurity standards and their implications for digital rights*
- *Copyright infringement in the age of AI*
- *Balancing privacy rights with public safety*
- *AI and algorithmic accountability*

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