FOUNTAINHEAD LEGAL

EDITION I - NOVEMBER 2024

TECHNOLOGY LAW AND DATA PRIVACY UPDATES

INDEX

A. PREFACE

B. NATIONAL

- Karnataka High Court Rules on Liability of Online Aggregators
- Madras High Court - Evidence obtained through Invasion of Spousal Privacy Inadmissible
- Digital Life Certificate 3.0 for Pensioners
- Bombay High Court rules out Defamation on mere receipt of WhatsApp Messages and pulls up Authorities for registering Offences under Section 66A of IT Act
- Kerela High Court Limits Media Trials in an Ongoing Criminal Litigation

C. INTERNATIONAL

Australia

- Australia releases Guidance for Businesses and Developers in AI Industry
- Australian Country Court recognises Invasion of Privacy under Tort

United States of America

- Tiktok accused of Children's Privacy Law Violation

European Union

- EU Ruling: Aligning Data Protection Laws with Competition Law

Canada

- Supreme Court Rules IP Address Protected Under the Canadian Charter Commission
- Public School Teachers Are Protected by Charter's Privacy Rights

D. ABOUT FOUNTAINHEAD LEGAL

E. CONTACT DETAILS

PREFACE

Welcome to the latest edition of Fountainhead Legal's Data Privacy and Technology Law newsletter.

In India, the Karnataka High Court has delivered a pivotal ruling on the liability of online aggregators, particularly in the ride-hailing sector. The Court held that platforms exercising significant control over drivers—such as setting fares and routes—cannot merely claim intermediary status under the Information Technology Act, 2000 ("**IT Act**"). This ruling redefines intermediary liability under Section 79, emphasizing platform accountability for user safety.

Additionally, the Madras High Court reinforced spousal privacy as a fundamental right, barring evidence obtained through privacy violations. The Bombay High Court highlighted the importance of adhering to judicial precedents, criticizing the misuse of outdated IT Act provisions. Meanwhile, the Kerala High Court cautioned against media trials that could compromise fair trial rights.

On the international front, Australian has introduced new privacy guidelines for AI whereas the Court has recognized invasion of privacy as a legal tort. The U.S. Federal Trade Commission has filed a lawsuit against TikTok for violating children's privacy laws and breaching a 2019 consent order requiring stricter privacy practices. In the EU, GDPR enforcement has been bolstered by allowing competitors to challenge violations as unfair trade practices. Canada's Supreme Court has ruled that IP addresses and teacher communications are protected under its Charter.

Globally, courts and governments are advancing privacy laws to keep pace with technological growth, urging organizations to align with evolving standards. These developments underscore the global recognition of the need to strengthen data protection frameworks and uphold privacy rights in an increasingly digital world. From judicial pronouncements that redefine privacy norms to legislative measures driving compliance, the focus remains on balancing innovation with accountability.

At Fountainhead Legal, we are committed to guiding organizations through this dynamic landscape. With our deep expertise in data privacy compliance and a nuanced understanding of regulatory frameworks, we offer tailored solutions to meet each client's unique needs. Whether it's drafting privacy policies, building data protection frameworks, advising on cross-border data transfers, or delivering employee training programs, our team is equipped to support every step of your compliance journey.

We hope you find this edition insightful and informative!

NATIONAL

1. Karnataka High Court rules on Liability of Online Aggregators

On September 30, 2024, the High Court in the matter of *(X) v. Internal Complaints Committee, AniTechnologies Pvt. Ltd. [Writ Petition No. 8127 of 2019]*[1] has clarified the legal responsibilities of online aggregators, specifically in the context of ride-hailing services. The case stemmed from a passenger's complaint about harassment during a ride, leading to a legal battle over the cab aggregator's role as an 'intermediary' under the IT Act. The cab aggregator had claimed it merely facilitated connections between drivers and passengers, but the Court disagreed, finding that the platform exercises significant control over drivers, including determining fares, routes, and managing communications through its app.

The Court's judgment shifts the legal landscape for e-commerce and aggregator platforms, challenging the traditional interpretation of intermediary liability. While intermediaries are generally shielded from liability, the Court emphasized that the cab aggregator's operational control over drivers exceeded mere facilitation, thereby holding the platform accountable for ensuring user safety.

2. Madras High Court: Evidence obtained through Invasion of Spousal Privacy Inadmissible[2]

On October 30, 2024, High Court at Madras, in the matter of *R v. B [CRP(MD) No. 2362 of 2024]*, held that spousal privacy is a fundamental right protected under Article 21 of the Constitution of India. The case involved a husband who sought to submit a call data record (**"CDR"**) of his wife as evidence in a divorce petition, alleging cruelty and adultery. The Court ruled that the CDR, obtained without the wife's consent, was inadmissible, as it violated her right to privacy. The husband's submission failed to meet the statutory requirements for the admissibility of electronic records under Section 65B of the Evidence Act, 1872, as the certificate required for such evidence was not issued by an authorized official.

The Court emphasized that privacy, as affirmed in the landmark K.S. Puttaswamy judgment, cannot be violated unless done in accordance with a lawful procedure. It also noted that there is no specific legislation or 'regime of law' currently addressing privacy rights, making evidence obtained through the violation of privacy inadmissible in courts. Further, the Court stressed that marital misconduct does not justify illegal surveillance or snooping by one spouse on the other. Consequently, the Court set aside the lower court's order and reinforced the protection of spousal privacy as a fundamental right.

The increasing number of precedents in the area of personal privacy will not only help to change the mindset but also make the statutory implementation easy.

3. Digital Life Certificate 3.0 for Pensioners[3]

As part of its commitment to enhancing accessibility for pensioners, Department of Pension and Pensioners' Welfare is conducting the Nationwide Digital Life Certificate Campaign 3.0., an initiative that leverages 'Face Authentication' technology to simplify the submission of life certificates for pensioners. Pensioners can now submit their life certificates digitally using Aadhaar-based Face

[1] https://karnatakajudiciary.kar.nic.in/newwebsite/rep_judgmentcase.php
[2] https://mhc.tn.gov.in/judis/
[3] https://pib.gov.in/PressReleasePage.aspx?PRID=2071463

Authentication on Android smartphones, eliminating the need for biometric devices or physical visits to Pension Disbursing Authorities.

4. Bombay High Court rules out Defamation on mere receipt of WhatsApp Messages and pulls up Authorities for registering Offences under Section 66A of IT Act

The Bombay High Court, in *Ashwinkumar Pandhari Sanap v. State of Maharashtra [Criminal Application No. 2908 of 2024]*[4], delivered a significant ruling clarifying that recipients of WhatsApp messages are not liable for defamation unless they actively forward or publish the content. Highlighting the privacy afforded by end-to-end encryption, the Court ruled that a message only visible to the recipient, does not constitute defamation unless shared further. The applicant was arrested based on an FIR filed by his ex-wife's brother, alleging defamation via a WhatsApp message invoking Sections 66-A, 66-B, and later 67-A of the IT alongside Section 500 of the Indian Penal Code, 1860.

While examining the issue of defamation, the Court reiterated that registering offences under Section 66A of the IT Act which was declared unconstitutional by the Supreme Court in *Shreya Singhal v. Union of India [AIR 2015 SC 1523]* is illegal. The Court emphasized that despite the striking down of Section 66A, its continued invocation violates judicial precedent and legal sanctity.

The judgment provides clarification that a private WhatsApp message does not amount to defamation unless actively forwarded or published recognizes the protective shield of end-to-end encryption, safeguarding individual privacy. This distinction is crucial in an era where digital communication is often misinterpreted as public dissemination. It also emphasizes on the responsibility of law enforcement agencies to strictly comply with the Supreme Court's directives and refrain from registering cases under invalid provisions like Section 66A of the IT Act. It serves as a crucial reminder of the need for compliance and vigilance in cases involving IT Act provisions. Notably, this is not the first instance where authorities have invoked Section 66A despite its repeal, highlighting the urgent need for enhanced awareness and training to ensure adherence to the law.

5. Kerela High Court limits Media Trials in an Ongoing Criminal Litigation

The Kerela High Court rules on media trials while emphasizing on the right to privacy of an individual in the case of *Dejo Kappan v. Deccan Herald & Ors [2024: KER:82715]*[5], wherein the petitioner filed a defamation suit against the Deccan Herald and other connected parties, alleging that false and defamatory reports were published about him, damaging his reputation. The petitioner contended that the news articles misrepresented facts and accused him of criminal activities without substantiated evidence.

The Court held that while the media enjoys the freedom of speech and expression, it must exercise caution and due diligence in verifying facts before publishing to prevent defamation. The Court warned that such unchecked reporting can infringe on the accused's right to a fair trial and compromise public trust in the justice system. While recognizing the media's duty to inform, the Court urged control in expressing opinions on cases still under investigation, stressing that any overreach violates the constitutional right to privacy and dignity under Article 21. It ruled that the media's right to publish does not extend to infringing upon an individual's privacy or spreading false information that harms

[4] https://bombayhighcourt.nic.in/
[5] https://hckinfo.kerala.gov.in/digicourt/Casedetailssearch

their reputation. The Court thus ordered the respondents to pay damages for the harm caused, reinforcing the balance between the freedom of the press and the protection of individual rights.

INTERNATIONAL

AUSTRALIA

1. Australia releases Guidance for Businesses and Developers in AI Industry

Recently, the Office of Australian Information Commissioner released two sets of guidelines – *Guidance on privacy and the use of commercially available AI products*[6] and *Guidance on privacy and developing and training generative AI models*[7] to assist entities using AI models/systems as well as developers of AI models/systems to comply with their obligations under the Privacy Act, 1988 and Australian Privacy Principles guidelines to navigate legal landscape in a responsible manner.

For businesses using AI, these guidelines emphasise on conducting due diligence on AI providers, ensuring data minimization by using only necessary information, being transparent in their privacy polices about use of AI and make disclosures regarding data generated through AI. Developers are to minimize personal data use in training datasets, prioritize lawful and transparent data collection, and ensure de-identification of data to mitigate privacy risks. Guidelines recommend both, businesses and developers to conduct Privacy Impact Assessment to identify risks associated with privacy to promote 'privacy by design' approach in AI industry.

2. Australian Country Court recognises Invasion of Privacy under Tort

In the matter of *Waller Lynn (pseudonym) v. Barrett Romy (pseudonym) [2024] VCC 962*[8], a daughter filed case against her father on multiple grounds including invasion privacy by disclosing sensitive information relating to her mental health that she had shared during counselling session. The information was shared via private emails to news providers and disclosed in defendant's book. This was examined thoroughly by the court to understand whether actionable claim for privacy exists under common law or not.

It was held that an actionable claim for invasion of privacy exists under common law in Australia, marking a significant step in the recognition of privacy as a fundamental legal right. Drawing on domestic and international legal developments, the judge explained that privacy claims could build upon existing legal principles designed to protect confidential information, while explaining the difference between 'privacy' and 'confidentiality'. Applying this reasoning to the case, the Court found that the disclosure of false information namely, an email shared by defendant that inaccurately implied that applicant had apologized, constituted a breach of privacy as the email in question violated daughter's privacy and dignity because it was shared in a way that created a false impression of her actions. This misrepresentation not only disclosed private correspondence without her consent but also distorted its meaning, potentially harming her reputation and personal integrity.

The court emphasized that the violation lay not merely in the content, but, in the intrusion into the applicant's private sphere and dignity. After balancing this against the defendant's free speech rights, the court awarded applicant AU $30,000 in damages, highlighting the need to uphold privacy values while fostering the development of this nascent tort.

[6] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-the-use-of-commercially-available-ai-products

[7] https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/guidance-on-privacy-and-developing-and-training-generative-ai-models

[8] https://austlii.edu.au/cgi-bin/viewdoc/au/cases/vic/VCC/2024/962.html#

UNITED STATES OF AMERICA

1. Tiktok accused of Children's Privacy Law Violation[9]

Tiktok faces a lawsuit by Department of Justice (**"DOJ"**) for violation of Children's Online Privacy Protection Act, 1998 (**"COPPA"**). Tiktok was accused of collecting personal data from children under 13 without obtaining verifiable parental consent, failing to safeguard that data, and continuing these practices despite being under a 2019 consent order requiring enhanced compliance. It is claimed that TikTok ignored recurring privacy concerns, demonstrating a disregard for its obligations under COPPA. It was further alleged that Tiktok built back doors on its platform to allow children to use its platform without undergoing the strict screening process required for children and also used children's data for targeted advertisement. A penalty of USD $51,744 per violation, per day has been imposed.

The ongoing lawsuit against TikTok following allegations of COPPA violations, is yet another instance highlighting concerns over the TikTok's data protection practices, especially regarding children. Previous fines imposed in the European Union and the United Kingdom further amplify these concerns and call into question whether TikTok, as a global company, adequately prioritizes the security and privacy of its young users. Handling children's data necessitates robust mechanisms, including verifiable parental consent, as children are often unaware of the risks associated with using such platforms. Ensuring stricter compliance is vital to safeguard children from targeted advertisements and unauthorized data use, underscoring the responsibility of companies like TikTok to uphold the highest standards of data protection.

EUROPEAN UNION

1. EU Ruling: Aligning Data Protection Laws with Competition Law[10]

In October 2024, the Court of Justice of the European Union ("**CJEU**") delivered a landmark judgment, affirming that GDPR does not prevent EU Member States from enabling competitors to file civil lawsuits against organizations for GDPR violations under the prohibition of unfair commercial practices. Originating from a German case, this ruling recognizes that GDPR infringements, while primarily affecting data subjects, can also harm competitors by distorting market competition and breaching consumer protection rules. The CJEU emphasized that access to and use of personal data are critical competitive factors in the digital economy and that aligning data protection rules with competition law ensures fair market practices.

This decision enhances GDPR enforcement by allowing competitors to hold organizations accountable, potentially reshaping business strategies in competitive markets and prompting businesses to assess their risk of such actions in EU Member States.

[9] https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62023CJ0021

CANADA

1. Supreme Court Rules IP Address Protected Under the Canadian Charter[11]

The Supreme Court of Canada in *Andrei Bykovets v. His Majesty The King (R. v. Bykovets, 2024 SCC 6)* ruled that an individual's IP address is protected under Section 8 of the Canadian Charter of Rights and Freedoms, which safeguards against unreasonable search and seizure. The Court found that law enforcement must obtain judicial authorization before accessing an individual's IP address from a third-party provider, such as a payment processor, even in the context of a criminal investigation.

The ruling reflects the Court's recognition of the highly sensitive nature of information tied to an IP address, which can reveal extensive personal details about an individual's online activities.

2. Public School Teachers Are Protected by Charter's Privacy Rights[12]

The Supreme Court of Canada upheld the lower court's ruling which held that the Ontario public school teachers are entitled to privacy protections under the Canadian Charter of Rights and Freedoms, which guards against unreasonable search and seizure. The case involved two teachers whose private communications were accessed by a school principal without consent. The school board subsequently issued written reprimands based on these communications.

The Court dismissed the appeal from the School Board, affirming that public school teachers' rights to privacy in the workplace are protected under the Charter. The Court ruled that Ontario public school boards are considered 'Governmental' entities for the purposes of section 32 of the Canadian Charter, as public education is inherently a Governmental function. Therefore, all actions taken by public school boards, including those related to employee privacy, are subject to Charter scrutiny.

[11] https://www.canlii.org/en/ca/scc/doc/2024/2024scc6/2024scc6.html
[12] https://www.canlii.org/en/ca/scc/doc/2024/2024scc22/2024scc22.html

ABOUT FOUNTAINHEAD LEGAL

Fountainhead Legal is an emerging law firm specializing in key practice areas such as indirect taxation (including customs duty, GST and erstwhile indirect tax legislations), general corporate law, data privacy & technology law along with family and succession matters. The firm's team of experienced and dynamic young lawyers blends deep legal expertise with fresh perspectives, delivering innovative, solution-oriented legal counsel. This synergy of knowledge and energy ensures clients receive forward-thinking advice tailored to their unique needs.

Rashmi Deshpande, the founder of Fountainhead Legal, is a seasoned professional with 18 years of experience in Big 4 consulting and leading law firms. She launched Fountainhead Legal in 2023 after serving as a Partner at Khaitan & Co. Her expertise spans a wide array of industries, including Life Sciences, Insurance, IT/ITES, EPC, Financial Services, and Real Estate.

Despite its recent inception, Fountainhead Legal has quickly gained recognition as a leading authority in data protection, providing businesses with comprehensive compliance solutions. The firm's services include drafting privacy policies, offering expert opinions on data privacy and security practices, and developing robust compliance frameworks. Fountainhead Legal has been instrumental in keeping organizations ahead of evolving regulatory requirements by providing regular updates and expert guidance.

For More Information - Contact Details:

Rashmi Deshpande

Email: rashmi@fountainheadlegal.com

Contact Number: +91 98338 62234

Aarushi Ghai

Email: aarushi@fountainheadlegal.com

Contact Number: +91 91314 15290

Janmejay Jaiswal

Email: janmejay@fountainheadlegal.com

Contact Number: +91 98190 42239

Fountainhead Legal

Address: C-2106, Oberoi Garden Estate,

Chandivali Farm Road, Powai - 400072

Website: https://fountainheadlegal.com/

LinkedIn: https://www.linkedin.com/company/fountainhead-legal/