EDITORIAL

Regulating Artificial Intelligence (AI)

In this special edition of the Global Privacy Law Review (GPLR), we embark on a journey to explore the legal implications of artificial intelligence (AI) and navigate the evolving confluence with various legal frameworks, including privacy and data protection.

AI is rapidly transforming the legal landscape, and it is essential that we examine the implications of this technology for our legal system. We have therefore assembled a distinguished group of authors to provide insight into the legal and policy considerations of AI. Each article and report in this special edition sheds light on the complexities that define the intersection of technology and law.

In the peer-reviewed *Articles* section, Javier Torre de Silva y López de Letona analyses the right to scrape data on the internet, an increasingly popular method for gathering data from the web to train and build generative AI systems.[1] In particular, he considers the legality of web scraping in the light of the recent rulings in *hiQ Labs, Inc. v. LinkedIn Corp.* in the US.[2]

Torre de Silva's article transcends a mere exploration of web scraping. His comprehensive analysis scrutinizes the various court rulings and also unveils the broader implications for data ownership, innovation, and the delicate balance between fostering creativity and safeguarding proprietary data.

hiQ Labs v. LinkedIn has an unusual legal posture and a complex history spanning six years.[3] The case began in 2017 when LinkedIn threatened hiQ, a small data analytics company that used automated bots to scrape data from public LinkedIn profiles, with legal action for violating the US Computer Fraud and Abuse Act of 1986 (CFAA).

The CFAA is the federal anti-hacking statute prohibiting access to computers and networks 'without authorization' (or in excess of 'authorized access').[4] Since data scraping is not per se unlawful, organizations rely on the CFAA to protect that data. However, the term 'without authorization' is not defined, leaving it to the courts to decide how this should be applied.

In addition, LinkedIn implemented technical measures designed to restrict hiQ's automated access and collection of LinkedIn profile data.

hiQ responded by suing LinkedIn in federal court for anti-competitive conduct, arguing that[5]:

> public data must remain public and innovation on the internet should not be stifled by anti-competitive hoarding of public data by a small group of powerful companies.

Further, hiQ scored an initial victory by obtaining a preliminary injunction from the district court forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles in 2017.[6]

In September 2019, the Ninth Circuit agreed with the district court that hiQ had no viable way to remain in business without using LinkedIn's public data and therefore was likely to suffer irreparable harm.[7] The Ninth Circuit stated:

> the CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. It is likely

Notes

1 Javier Torre de Silva y López de Letona, *The Right to Scrape Data on the Internet: From the US Case hiQ Labs, Inc. v. LinkedIn Corp. to The ChatGPT Scraping Cases – Differences Between US and EU Law*, in this issue at 5.

2 *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 9th Cir. 2019.

3 Lee Gesmer, *LinkedIn Cannot Use the CFAA To Stop Scraping of Its Public Facing Web Data*, LinkedIn (28 Jul. 2022), www.linkedin.com/pulse/linkedin-cannot-use-cfaa-stop-scraping-its-public-facing-lee-gesmer (accessed 17 Jan. 2024).

4 18 USC §1030(a)(2) CFAA.

5 Andrew Chung, *US Supreme Court Revives LinkedIn Bid to Shield Personal Data*, Reuters (14 Jun. 2021), www.reuters.com/technology/us-supreme-court-revives-linkedin-bid-shield-personal-data-2021-06-14 (accessed 17 Jan. 2024).

6 *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, Dist. Court, N.D. California 2017.

7 *See hiQ Labs, Inc. v. LinkedIn Corp., supra* n. 2.

> that when a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA. The data hiQ seeks to access … has not been demarcated by LinkedIn as private using … an authorization system. hiQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim.

This key ruling (which the Ninth Circuit reaffirmed in April 2022[8] following a remand from the US Supreme Court in light of *Van Buren*[9]) narrowed the scope of the CFAA by concluding that the CFAA did not prohibit the automated scraping of publicly accessible data.[10]

The decision was seen as a victory for data analytics companies and researchers who use bots to scrape information from public-facing websites, as it established a legal precedent that could be used to protect the right to scrape data from the web in the future.

However, in a mixed ruling dated 4 November 2022, a California district court ruled that hiQ had breached LinkedIn's User Agreement by scraping and using scraped data.[11]

In early December 2022, the parties in the long-running litigation eventually reached a confidential settlement agreement.[12]

While this dispute is resolved, many of the questions in the case remain unanswered. Thus, issues related to web scraping and the validity of claims under the CFAA and breach of contract, among others, are likely to emerge in other cases. This has already happened in a series of outstanding court proceedings such as *Meta Platforms, Inc. v. Bright Data Ltd.*[13] and *Ryanair DAC v. Booking Holdings Inc.,*[14] as discussed by Torre de Silva.[15]

Nonetheless, the hiQ rulings seem to endorse, at least in some circumstances, the scraping of publicly available websites without fear of liability under the CFAA in the US.

Torre de Silva also compares this outcome with the European Union (EU) position and analyses the lawfulness of web scraping in accordance with EU law, under criminal, privacy and data protection, copyright and sui generis rights, and contract laws.[16] He concludes that the EU position is 'substantially different' from the US outcome.[17]

In the second article, Camilla Della Giustina & Pierre de Gioia Carabellese explore the ethical and legal nuances surrounding AI in law enforcement.[18]

This article delves into the *R v. Chief Constable of South Wales* case in the UK, providing readers with an analysis of the legal intricacies, potential biases, and societal implications of deploying AI-driven facial recognition in policing.[19]

The analysis extends beyond the courtroom, positioning the legal discourse within the broader context of evolving norms around privacy, civil liberties, and the transformative impact of technology on law enforcement.

In *R v. Chief Constable of South Wales*, the Court of Appeal Civil Division unanimously held that the South Wales Police's (SWP's) use of 'automatic facial recognition locate' technology violated the right to privacy under Article 8 of the European Convention on Human Rights (ECHR), the United Kingdom Data Protection Act and the Public Sector Equality Duty.

The court also ruled that the SWP could not demonstrate that the use of such technology has no detrimental effect on the rights of the public or that it did not have the potential to produce discriminatory effects.

This ruling serves as a touchstone, provoking broader discussions on responsible AI governance. Its considerations of necessity, proportionality, and individual rights echo globally, leaving an indelible mark on the delicate equilibrium between public safety imperatives and the preservation of fundamental rights.

Della Giustina and de Gioia Carabellese also review the case law of the European Court of Human Rights in relation to Article 8 of the ECHR.

Notes

8 *hiQ Labs, Inc. v. LinkedIn Corp.*, Court of Appeals, 9th Circuit 2022.

9 *Van Buren v. United States*, 141 S. Ct. 1648, Supreme Court 2021.

10 Alex Reese & Raven Quesenberry, *What Recent Rulings in 'hiQ v. LinkedIn' and Other Cases Say About the Legality of Data Scraping*, The Recorder (Farella Braun + Martel LLP) (22 Dec. 2022), www.fbm.com/publications/what-recent-rulings-in-hiq-v-linkedin-and-other-cases-say-about-the-legality-of-data-scraping (accessed 17 Jan. 2024).

11 *hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17–3301, ND California (4 Nov. 2022).

12 Jeffrey D. Neuburger, *hiQ and LinkedIn Reach Proposed Settlement in Landmark Scraping Case*, New Media and Technology Law Blog (8 Dec. 2022), www.natlawreview.com/article/hiq-and-linkedin-reach-proposed-settlement-landmark-scraping-case (accessed 17 Jan. 2024).

13 *Meta Platforms, Inc. v. Bright Data Ltd.*, 3:23-cv-00077 (N.D. Cal.).

14 *Ryanair DAC v. Booking Holdings Inc.*, No. 20–01191 (D. Del. 24 Oct. 2022).

15 Torre de Silva, *supra* n. 1.

16 *Ibid.*, at 13.

17 *Ibid.*, at 22.

18 Camilla Della Giustina & Pierre de Gioia Carabellese, *AI, Facial Recognition, and Policing: Business Opportunities and Legal Challenges – A UK Analysis With Glimpses of EU Law*, in this issue at 23.

19 *R (on the application of Edward Bridges) v. the Chief Constable of South Wales Police* [2020] EWCA Civ 1058.

The authors conclude by considering the restrictions and prohibitions on facial recognition set out in the upcoming EU AI Act.

In the *Reports* section, I further analyse the AI Act with an overview of this new regulatory framework set to govern AI systems in the EU.[20]

At the time of editing this issue, technical negotiations on the final text of the AI Act are ongoing, and we do not have a final consolidated text. My analysis in this report should therefore be seen as a preliminary introduction and may change depending on the final text.

In any event, the EU AI Act represents a leap toward regulating and harmonizing AI regulation across Member States. By addressing transparency, accountability, and human oversight, the proposed legislation seeks to strike a delicate (and difficult) balance between innovation and safeguarding fundamental rights in our digital age.[21]

I hope that my overview will serve as a guide for understanding the potential impacts of the AI Act on the future development and deployment of AI technologies in the EU and provide the readers with insights into the Act's approach to transparency, accountability, and human oversight – critical components for stakeholders navigating the impending regulatory AI landscape.[22]

Similarly, in Asia, Esther Franks, Bianca Lee & Hui Xu of Latham & Watkins review three key AI-specific regulations enacted in the People's Republic of China (PRC) in 2022 and 2023.[23]

These regulations also set out comprehensive obligations on the use of generative AI and algorithmic recommendation services in the PRC.[24]

They lay down general requirements to ensure lawfulness and fairness and to protect against 'incorrect political direction and violation of social morality'.[25]

In India, there are also significant developments in technology law. The government recently proposed the enactment of the Digital India Act (DIA), an EU-like law to regulate Big Tech and create a safer digital space.

Durga Priya Manda & Anant Narayan Misra from AZB & Partners analyse the proposed DIA, which is intended to replace the existing Information Technology Act of 2000.[26]

As India aims to assert itself as a digital force, this report navigates the intricacies of the proposed DIA. Manda & Misra dissect key provisions, providing readers with a thorough understanding of India's evolving approach to regulating the digital sphere.

This report transcends mere legislative review, offering insights into how the proposed legislation addresses critical aspects of the rapidly evolving digital landscape – from online safety to a fair and open internet. Readers will gain a nuanced perspective on how India seeks to regulate online monopolies and balance technological growth with the protection of individual rights in the digital space.

Finally, in the *Book Review* section, Héctor Guzmán-Rodríguez of Bello, Gallardo, Bonequi y García (BGBG) reviews Mistale Taylor's Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality.[27]

Taylor's book provides a comprehensive analysis of the legal and policy implications of data protection law in the transatlantic context. She examines the challenges of balancing fundamental rights, privacy, and extraterritoriality in a rapidly changing digital world.

As Guzmán-Rodríguez notes, readers will find in Taylor's book an in-depth explanation of the EU's approach to protect, even beyond its boundaries, data subjects' personal data in the ambitious General Data Protection Regulation (GDPR).[28]

Understanding the legal intricacies and practical considerations surrounding international data transfers is essential for organizations operating in a globalized data environment.

I extend our gratitude to our authors and invite readers to immerse themselves in the profound insights presented in these articles, reports, and book review. I hope that this edition will provide a valuable resource for legal scholars, practitioners, and policy-makers as they grapple with the implications of AI as well as the intersection of technology and law.

Sincerely

Ceyhun Necati Pehlivan
Editor-in-Chief
Email: ceyhun.pehlivan@linklaters.com.

Notes

[20] Ceyhun Necati Pehlivan, *The EU Artificial Intelligence (AI) Act: An Introduction*, in this issue at 31.

[21] *Ibid.*, at 32.

[22] *Ibid.*, at 33.

[23] Esther Franks, Bianca Lee & Hui Xu, *China's New AI Regulations*, in this issue at 43.

[24] *Ibid.*, at 44.

[25] *Ibid.*, at 43.

[26] Durga Priya Manda & Anant Narayan Misra, *India To Replace Information Technology Act With The Proposed Digital India Act: Out With The Old, In With The New?*, in this issue at 50.

[27] Héctor Guzmán-Rodríguez, Review of *Transatlantic Jurisdictional Conflicts in Data Protection Law: Fundamental Rights, Privacy and Extraterritoriality, Mistale Taylor. Cambridge University Press: 2023. 271 pp. GBP 95. ISBN 978-1-108-48956-0*, in this issue at 54.

[28] *Ibid.*, at 54-55.