# EDITORIAL

## Editorial Note

As in each new edition, I am pleased to present the top-class articles, report, and case note published in this issue of Global Privacy Law Review (GPLR).

The *Articles* section contains two highly interesting and relevant articles.

First, Sultan-Mahmood Seraj (*Post-Pandemic Telehealth: An Unhealthy Privacy Prescription*) analyses the use of telehealth services across the United States (US) in the post-COVID-19 pandemic.[1]

The pandemic has catapulted telehealth as a substitute to traditional healthcare delivery methods to protect both patients and healthcare providers and reduce the burden on health systems.[2] In response to this public health emergency, the Office for Civil Rights (OCR) at the US Department for Health & Human Services (HHS) decided not to enforce the Health Insurance Portability and Accountability Act's (HIPAA's) requirements governing audio and video communication technologies.[3] Accordingly, OCR allowed healthcare providers to reach patients using common non-public facing video and messaging services, such as Apple FaceTime, Facebook Messenger, and Skype.[4]

OCR also announced that covered health care providers are not subject to penalties for violations of the HIPAA Privacy, Security, and Breach Notification Rules that occur 'in the good faith provision of telehealth during the COVID-19 nationwide public health emergency'.[5] For instance, if a provider suffers a cyberattack that exposes protected health information (PHI) from a telehealth session, it will not face HIPAA penalties.

In the US, federal agencies enjoy broad discretion in deciding whether to bring enforcement actions, and courts generally decline to review such decisions.[6]

Seraj argues that the US government has not adequately considered standardizing rules for remote telehealth consultations and regulating the flow of sensitive patient data in a post-COVID-19 world.[7] In his article, the author addresses key legal issues associated with telehealth services and recommends national standards to mitigate physician liability while prioritizing patient care.[8]

The second article focusses on South Asia. M. Toriqul Islam (*Legal Development for Privacy and Data Protection in Bangladesh*) offers an overview of the existing and upcoming privacy and data protection framework in Bangladesh.[9]

In this regard, Islam considers the latest developments in Bangladesh and, in particular, analyses the Data Protection Bill (Bill) proposed by the Information and Communication Technology (ICT) Division of the government of Bangladesh in 2022.[10] The author assesses whether these developments are adequate compared to relevant global standards, such as the European Union's (EU's) General Data Protection Regulation (GDPR).[11]

### Notes

1 Sultan-Mahmood Seraj, *Post-Pandemic Telehealth: An Unhealthy Privacy Prescription*, in this issue at 208.

2 Institute for Healthcare Improvement, *Telehealth*, https://www.ihi.org/Topics/Telehealth/Pages/default.aspx (accessed 21 Oct. 2022).

3 HHS, *Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency* (20 Jan. 2021), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html (accessed 21 Oct. 2022).

4 *Ibid.* However, public-facing video platforms, such as Facebook Live and TikTok, cannot be used to provide telehealth services.

5 HHS, *FAQs on Telehealth and HIPAA During The COVID-19 Nationwide Public Health Emergency*, https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf (accessed 21 Oct. 2022).

6 Congressional Research Service, *HIPAA, Telehealth, and COVID-19* (5 Jun. 2020), https://crsreports.congress.gov/product/pdf/LSB/LSB10490 (accessed 21 Oct. 2022).

7 Seraj, *supra* n. 1, at 208.

8 *Ibid.*

9 M. Toriqul Islam, *Legal Development for Privacy and Data Protection in Bangladesh*, in this issue at 221.

10 For an unofficial English translation of the proposed Data Protection Act 2022, *see* Government of the People's Republic of Bangladesh, Information and Communication Technology Division (16 Jul. 2022), https://ictd.portal.gov.bd/sites/default/files/files/ictd.portal.gov.bd/page/6c9773a2_7556_4395_bbec_f132b9d819f0/Data%20Protection%20Bill%20en%20V13%20Unofficial%20Working%20Draft%2016.07.22.pdf (accessed 21 Oct. 2022).

11 *Ibid.*

The Bill imposes, among others, data localization or data sovereignty requirements and restricts cross-border data transfers outside the country without prior government approval. Such requirements should be read in conjunction with the Bangladesh Telecommunication Regulation Act 2001, which confers broad powers to the government to intercept, record, or collect information of any person on national security or public order grounds.[12] As a result, the Bill has been widely criticized for threatening people's right to privacy in Bangladesh.[13]

In the *Report* section, Tanguy Van Overstraeten & Richard Cumbley (*Brace! Brace! Brace! The Wave of Incoming CJEU Decisions*) consider the large number of pending decisions on data protection matters in front of the Court of Justice of the EU (CJEU).[14]

Van Overstraeten & Cumbley note that the CJEU places great weight on protecting the rights of individuals and has not shied away from decisions that create significant practical difficulties for businesses.[15] Accordingly, businesses operating in the EU should 'brace for' significant change ahead.[16] The authors also consider the extent to which the courts of the United Kingdom will continue to follow decisions of the CJEU.[17]

Finally, in the *Case Note* section, Athanasios Kolovos & Janet K. Brewer analyse and draw a dystopian parallel between the California Supreme Court's decision in *People v. Buza*[18] and Andrew Niccol's science fiction thriller film *Gattaca.*[19,20]

In *People v. Buza*, the California Supreme Court upheld the state's Proposition 69 known as the DNA Fingerprint, Unsolved Crime and Innocence Protection Act (DNA Act) over constitutional challenges by Mark Buza. Buza had been arrested for arson and refused to provide a DNA sample by cheek swab. A jury later convicted him of both the arson-related felonies and the misdemeanour offense of refusing to provide a DNA sample required by the DNA Act. The Court of Appeal reversed defendant's misdemeanour refusal conviction, holding that the DNA Act violated his rights under the Fourth Amendment to the US Constitution. Nevertheless, while the case was pending on appeal, the US Supreme Court addressed a similar issue in *Maryland v. King*,[21] and held that:

> [w]hen officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.

Eventually, the California Supreme Court concluded that the DNA Act's collection requirement is valid as applied to Buza who was validly arrested on probable cause to hold for a serious offense.

Kolovos & Brewer discuss the constitutional concerns of the case and offer a discussion of social class and genetic engineering in light of *Gattaca.*[22] As most cinephiles will remember, *Gattaca* draws on concerns over reproductive technologies that facilitate eugenics, and the possible consequences of such technological developments for society.[23] The authors explore genetic privacy and non-discrimination laws and consider the sociological and legal implications if a situation similar to *Gattaca* were to occur in the future.[24]

*I hope you enjoy reading this new edition of the GPLR!*

*Ceyhun Necati Pehlivan*
*Editor-in-Chief*

## Notes

[12] Section 97(Ka) Bangladesh Telecommunication Regulatory Act 2001.

[13] *See* Nilesh Christopher, *Bangladesh's New Data Protection Law Grants More Power to the State Than Its People*, Rest of World (24 Aug. 2022), https://restofworld.org/2022/newsletter-south-asia-bangladeshs-data-protection-law (accessed 21 Oct. 2022), and Amnesty International, *Bangladesh: New Data Protection Bill Threatens People's Right to Privacy* (27 Apr. 2022), https://www.amnesty.org/en/latest/news/2022/04/bangladesh-new-data-protection-bill-threatens-peoples-right-to-privacy (accessed 21 Oct. 2022).

[14] Tanguy Van Overstraeten & Richard Cumbley, *Brace! Brace! Brace! The Wave of Incoming CJEU Decisions*, in this issue at 236.

[15] *Ibid.*

[16] *Ibid.*

[17] *Ibid.*

[18] *People v. Buza*, 197 Cal. App. 4th 1424 – Cal: Court of Appeal, 1st Appellate Dist., 2nd Div. 2011.

[19] Andrew Niccol (director and writer), *Gattaca*, Columbia Pictures & Jersey Films, 1997.

[20] Athanasios Kolovos & Janet K. Brewer, *People v. Buza*, in this issue at 243.

[21] *Maryland v. King* (2013) 569 US 435 [186 L. Ed. 2d 1, 133 S. Ct. 1958].

[22] Kolovos & Brewer, *supra* n. 20.

[23] Wikipedia, *Gattaca*, en.wikipedia.org/wiki/Gattaca (accessed 21 Oct. 2022).

[24] Kolovos & Brewer, *supra* n. 20.