Nr. 695E
19.06.2025

Jack Provan
Research Associate & PhD Student IFHV
Ruhr-Universität Bochum

NACHFRAGEN:
jack.provan@ruhr-uni-bochum.de

Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

IFHV

BOFAXE

et tu, U2? (Part 1)

Surveillance capitalism and the Las Vegas (data) Sphere

If you were using social media around September 2023, there's an excellent chance you've already seen images or videos of the newly opened Las Vegas Sphere, an 18,000-capacity music and entertainment venue which opened that month. The venue opened with a 5-month *U2* residency which drew in over 600,000 attendees, becoming one of the highest grossing concert residencies of all time. U2 fans lucky enough to attend one of these record-breaking shows were met with the Sphere's state-of-the-art visual and sound system, its near-panoramic indoor screen, various technological attractions, and an innocuous "facial recognition notice" above the entrance, emblazoning a warning that the venue uses facial recognition technology in line with its Privacy Policy.

That Privacy Policy, accessible online, lists biometric data (a class of sensitive personal data which includes facial features) alongside other personal information such as name, age and email address among the data it collects from concert-goers attending events at the venue (Section 1A). Further information provided to comply with the California Consumer Privacy Act reveals that biometric information "collected when visiting one of our venues" can be used for, among other purposes, "[advancing] our commercial or economic interests" (Section 8).

This blog post explores the legality of commercial biometric data processing, first by highlighting recent cases involving alleged misuse of biometric data by the Sphere's parent company, Madison Square Garden Entertainment Group (MSG), before drawing a comparison between the US and EU frameworks for biometric data protection. The purpose is not to provide a comprehensive overview – to that end, we will not discuss the ECHR, also applicable in Europe – but to discover whether the EU's General Data Protection Regulation (GDPR) would allow data processing of the kind seen by MSG.

Madison Square Garden Entertainment Corp and abuse of biometric data

MSG own several high-profile venues across the USA including Radio City Music Hall and New York's Madison Square Garden – and they are no stranger to controversy surrounding their biometric data usage. In October 2022, a New York lawyer was denied entry to a Knicks game and had his season ticket revoked when his name appeared on the venue's "exclusion list", nine days after his firm had filed a lawsuit against MSG in an unrelated matter. Around the same time, a lawyer working for a different firm was turned away at the door to Radio City, despite the fact that she was not involved in her firm's case against MSG.

These instances revealed that MSG was using facial recognition technology to blacklist lawyers working for firms involved in cases against it. According to NYT, MSG was using third-party technology to mine the websites of law firms involved in cases against the company for photos of their lawyers – and conducting facial recognition scans at the doors to its venues to identify and remove them from events. MSG representatives have defended the policy as a reaction to the "adversarial environment" caused by litigation.

In March 2023, several lawyers initiated a class action lawsuit alleging MSG of improperly utilising their biometric data to deter litigation against the company. Under New York law, the plaintiffs had to show that MSG sought to directly profit from collecting their biometric data and sharing it with the facial recognition service – as opposed to deriving some other benefit. Put another way, the law "explicitly permits the collection and sharing of biometric data for commercial purposes provided that the public is warned," as long as the data controller does not "profit from the *transaction itself*." On that basis, since MSG was not directly selling the data but instead purchasing a service, the case was thrown out in May 2024. It appeared that the "facial recognition notices" above Sphere entrances were enough to legally justify the exclusion policy. Since then, a Bill has been introduced to the New York Senate which, if enacted, would establish a taskforce to identify the regulatory and ethical concerns around facial recognition technology. A much more comprehensive 2023 New York City Council Bill which would have banned the use of facial recognition technology in places of public accommodation, failed to reach enactment despite strong support from civil rights groups.

VERANTWORTUNG: Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, Massenbergstraße 11, 44787 Bochum, Tel.: +49 (0)234/32-27366, Fax: +49 (0)234/32-14208, Web: http://www.ruhr-uni-bochum.de/ifhv/. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de. **FÜR DEN INHALT SIND DIE JEWEILIGEN AUTORINNEN UND AUTOREN ALLEIN VERANTWORTLICH.**

Nr. 695E
19.06.2025

Jack Provan
Research Associate & PhD Student IFHV
Ruhr-Universität Bochum

NACHFRAGEN:
jack.provan@ruhr-uni-bochum.de

Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

IFHV

BOFAXE

et tu, U2? (Part 2)

Surveillance capitalism and the Las Vegas (data) Sphere

Biometric data protection in the USA and Europe

While the MSG exclusion policy seems to currently only apply to lawyers, CEO James Dolan has indicated in the past that he sees anyone who acts "confrontational [...] with the ownership" as fair game, implying a broad approach which could foreseeably lead to bans for all sorts of people who take issue with the company's business practices. There are already scant and anecdotal reports of fans who claim to have struggled to access MSG venues after criticising Dolan on social media.

The upshot of the failed New York lawsuit is that the law has remained one step behind the development of invasive surveillance technologies and their use by private companies. This is generally reflective of the wider legal progress on data protection, particularly in the US, where there is no comprehensive federal-level data privacy law equivalent to the EU's GDPR
Data protection law in the US is splintered by the nature of the data and is often left up to individual states. There are federal laws governing health data (HIPAA) and online privacy for children under 13 (COPPA), among others. At a state level, while many states remain broadly unregulated, few states have already introduced general data protection laws. States like Illinois, Texas and Washington have been particularly proactive in developing biometric data protection laws. In Illinois, this law establishes a private right of action which has seen fines of up to $75 million USD awarded in class action lawsuits against companies found to be misusing biometric data.

This fragmented approach to data protection stands in contrast to the EU, where the GDPR carves out special protections for biometric data. Article 9 prohibits the processing of "special categories" of data (including biometric), with a list of enumerated exceptions. Among those are with the explicit consent of the data subject (Article 9(2)(a)) and data which are already made public by the data subject (Article 9(2)(e)). While the CJEU has recently confirmed that personal data may be processed by for-profit organisations on the basis of legitimate commercial interests, that decision related to non-sensitive data (Article 6), which is far less tightly regulated. Indeed, Article 9 governing biometric data makes no mention of legitimate interests – referring only to the "legitimate activities" of non-profit organisations.

So, what about consent, or public information? Ordinarily, data subject consent sought under GDPR must be freely given, specific, informed and unambiguous (recital 32). This means, among other things, consent given by a 'clear, affirmative act' and with knowledge of its processing purposes. While whether or not walking through the entrance to a venue could be considered a clear, unambiguous granting of consent is perhaps debatable, biometric data enjoys extra protection that requires *explicit* consent, meaning consent given expressly by written or digital confirmation. More problematic could be the allowance of sensitive data processing where the data subject has made that data public themselves. If our facial images are mined from our employers' websites, or our Facebook pages, would this give free reign to their processing?

Very little guidance has been published on Article 9(2)(e). Even though facial images are considered biometric, and therefore, sensitive data (recital 14), the manifestly already-public nature of what our faces look like makes this information virtually impossible to obscure from the public, especially in the digital age. However, the use of facial recognition technology under GDPR is still subject to the additional requirements in Article 6, must be pursuant to the data processing principles enumerated in Article 5, and is restricted by Article 22 governing automated individual decision-making. Article 22 seems to offer the clearest protection in this context, as data subjects are protected from automated profiling with very few exceptions. Those exceptions include explicit consent (discussed above), and when the processing is authorised by law in a way which protects the freedoms and legitimate interests of the data subject. Read alongside Article 5, which restricts lawful data processing to that which is fair, transparent, and pursues a legitimate purpose, it does not seem likely that facial recognition-operated blanket bans would qualify as lawful under GDPR, nor that individual EU Member States could lawfully authorise it.

VERANTWORTUNG: Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, Massenbergstraße 11, 44787 Bochum, Tel.: +49 (0)234/32-27366, Fax: +49 (0)234/32-14208, Web: http://www.ruhr-uni-bochum.de/ifhv/. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de. **FÜR DEN INHALT SIND DIE JEWEILIGEN AUTORINNEN UND AUTOREN ALLEIN VERANTWORTLICH.**

Nr. 695E
19.06.2025

Jack Provan
Research Associate & PhD Student IFHV
Ruhr-Universität Bochum

NACHFRAGEN:
jack.provan@ruhr-uni-bochum.de

Völkerrechtsblog
INTERNATIONAL LAW & INTERNATIONAL LEGAL THOUGHT

IFHV

BOFAXE

et tu, U2? (Part 3)

Surveillance capitalism and the Las Vegas (data) Sphere

Rolling Out More Spheres?

Despite hiding behind their status as private companies, large corporations in charge of iconic venues like MSG are providing places of public accommodation – whether it be for sports, music, or any other public entertainment. Within those venues, civil and human rights (including but not limited to data protection) should be applied in how the owners interact with the public. MSG's prevalence in the events space may soon spread internationally with their plans to roll out more Spheres in countries such as Dubai and South Korea. Their first proposal, for London, was ultimately rejected after a long public consultation period wherein it was decided that local residents did not want 1.2 million LED lights shining advertisements through their bedroom windows throughout the night. For those residents in cities which may soon be welcoming their own Spheres, a final note of warning about their prospects of entry should they choose to be publicly critical of James Dolan and MSG: *Achtung, Baby!*

VERANTWORTUNG: Die BOFAXE werden vom Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht der Ruhr-Universität Bochum herausgegeben: IFHV, Massenbergstraße 11, 44787 Bochum, Tel.: +49 (0)234/32-27366, Fax: +49 (0)234/32-14208, Web: http://www.ruhr-uni-bochum.de/ifhv/. Bei Interesse am Bezug der BOFAXE wenden Sie sich bitte an: ifhv-publications@rub.de. **FÜR DEN INHALT SIND DIE JEWEILIGEN AUTORINNEN UND AUTOREN ALLEIN VERANTWORTLICH.**