

Turning biometrics into a commodity raises privacy and governance risks

Ángel Judel, José M. Muñoz, Carlos Amunátegui Perelló, Diego Borbón, José Antonio Iglesias, José Ángel Marinero, Natalia Monti, Moisés Sánchez, Ciro Colombara, Amanda de la Fuente & Aldo Díaz

 Check for updates

Paying people for their biometrics raises complex ethical and legal questions about consent, privacy and the long-term risks of handing over irrevocable personal data. This Comment examines why such models require caution and what safeguards could better protect the public.

Recent years have seen the emergence of large-scale biometric data collection models that offer financial incentives to participants. These initiatives aim to build extensive databases for identity verification, artificial intelligence training or digital authentication. However, recent court and regulatory decisions suggest a growing concern about whether such practices adequately protect privacy and other fundamental rights.

In Chile, the Supreme Court issued in 2025 the first judicial decision of its kind, ordering the deletion of a minor's iris data after finding that consent had been inadequate and privacy rights had been infringed¹ (we, the authors of this Comment, were involved in this case either as authors of amicus curiae briefs or as members of the legal team representing the claimant). The defendant company rejected this line of criticism, [maintaining](#) that its technology incorporates privacy-preserving features that ensure anonymity and compliance with applicable data protection law, and that the personal data used to generate a profile are retained and stored on the individual's own device rather than by the application or by third parties. In the Chilean case, these arguments were rejected by the Supreme Court, whose judgment is final and not subject to appeal.

In Europe, data protection authorities have taken precautionary or corrective measures in response to large-scale biometric data collection practices. In 2024, the Spanish Data Protection Agency (AEPD) ordered the suspension of certain biometric data collecting and processing activities – as well as the blocking of existing data – following complaints related to transparency, consent and the protection of minors². The involved company sought a judicial stay of the measure, but the Spanish courts rejected the request and [upheld the lawfulness](#) of the authority's decision. The precautionary court order became final, accompanied by a legally binding [commitment from the company](#) not to resume its operations in Spain until a definitive decision is issued by the Bavarian data protection authority. That same year, the Bavarian State Office for Data Protection Supervision (BayLDA) required corrective measures to ensure compliance with the European Union's General Data Protection Regulation (GDPR), including stronger consent procedures and the deletion of data collected without



a valid legal basis³. The company [announced](#) its intention to appeal the decision before the German courts.

These developments point to broader issues that extend beyond any single case. When biometric data – which are unique and effectively irreversible – are collected at scale and exchanged for financial compensation, new risks may arise for privacy, meaningful consent and long-term governance. This Comment examines the key concerns associated with pay-for-biometrics models and outlines policy questions that regulators and policymakers may need to address.

Four main concerns with biometric data as a commodity

The growing use of financial incentives to collect biometric data raises several concerns that go beyond individual cases. These concerns stem from the distinctive nature of biometric information, the conditions under which consent is obtained and the scale at which these systems operate.

First, biometric data are fundamentally different from most other forms of personal information. They are unique and effectively irreversible, and they can potentially be used for unambiguously identifying a person in different environments beyond their control⁴. In particular, ocular iris data collection poses risks such as: (1) the eventual collection of additional biometric data without notifying the user; (2) the possibility of reversing the encrypted numerical data and obtaining the original biometric data⁵; and (3) the collection of data related to the user's [race or gender](#) and personality⁶, among other sensitive information, without informing the user.

Second, the presence of financial incentives raises questions about whether consent can truly be considered free and informed. When individuals are offered payment in exchange for highly sensitive data, economic need or informational asymmetries may influence their decision. These concerns may be particularly important for vulnerable populations, including minors or individuals with limited understanding of the long-term implications of biometric data sharing. Moreover, the processing of personal data ought to serve a legitimate and clearly defined purpose. Compensation alone may not always constitute sufficient justification for the processing of highly sensitive and irreversible biometric data. Given the unique and permanent role that biometric data have in identifying individuals, their treatment as objects of commercial exchange raises complex legal and ethical questions. Consent to process such data ought to be grounded in a legitimate processing purpose under applicable data protection frameworks.

Third, it is important that those who rely on consent to process personal data be able to demonstrate that consent was freely given and that the decision would not have been different in the absence of financial incentives. The presence of monetary compensation may influence individuals' willingness to provide particularly sensitive data. This raises the need for clear regulatory criteria to assess the validity of consent in situations that involve vulnerable or marginalized populations, substantial information asymmetries, or potentially deceptive or opaque data collection practices. It also highlights the importance of specific protection measures for children and adolescents.

Finally, because biometric data are highly sensitive and effectively irreversible, their collection requires careful safeguards. In practice, this means that data collection should be carried out for a legitimate purpose, using personalized procedures, and with highly trained personnel who are capable of explaining the associated risks at a level appropriate to each user's understanding. By contrast, large-scale collection efforts that involve millions of individuals across multiple countries (particularly in public spaces) may lack the conditions necessary to ensure adequate privacy protection. Under internationally recognized data-protection standards, the processing of sensitive data is expected to follow core principles, including lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability.

Key questions

The emergence of large-scale pay-for-biometrics models raises several questions that regulators and policymakers may need to address⁷.

- (1) How should the large-scale collection of unique and irreversible biometric data be assessed? The collection of biometric data from millions of individuals worldwide, often in public spaces and through privately controlled devices, may amount to the global-scale mechanization of the capture of unique personal data that individuals cannot change or recover.
- (2) Should the commercialization of highly sensitive biometric data be restricted or prevented? The exchange of financial compensation for biometric data raises concerns about the use of such data to train private artificial intelligence systems for purposes that may be opaque or insufficiently defined.
- (3) How should regulators address the concentration of irrevocable biometric data within complex corporate structures? The storage and processing of such data within global networks controlled by one or a few operators may challenge existing frameworks of

oversight and accountability and may affect the public-law understanding of personal identity⁸.

- (4) How should national and international supervisory authorities evaluate the development of private global identification systems based on biometric data? Large-scale biometric collection initiatives may enable the creation of private systems of personal recognition that function as alternatives to public identification infrastructures.

Special considerations for children and adolescents

Particular attention may be required in relation to children and adolescents. Although the psychological and social consequences of risks such as identity theft have been studied in other vulnerable groups⁹, the collection of biometric data from minors raises additional concerns due to their dependence, limited capacity to assess long-term risks, reduced ability to exercise meaningful choice, the free development of their personality, and the irrevocable and irrecoverable nature of biometric data in the future.

According to the Article 29 Data Protection Working Party, the predecessor of the current European Data Protection Board (EDPB): "[t]he use of biometrics could impact significantly on the dignity, privacy and the right to data protection of vulnerable people such as young children ... Given the potentially harmful consequences for the persons concerned, more stringent requirements will have to be met in the impact assessment process of any measure interfering with an individual's dignity"¹⁰.

These considerations highlight the importance of careful oversight when large-scale biometric data collection initiatives include or may affect children and adolescents.

Ángel Judel¹, **José M. Muñoz**^{1,2,3,4}✉, **Carlos Amunátegui Perelló**^{1,5}, **Diego Borbón**⁶, **José Antonio Iglesias**⁷, **José Ángel Marínaro**^{1,8}, **Natalia Monti**⁹, **Moisés Sánchez**¹⁰, **Ciro Colombara**^{10,11}, **Amanda de la Fuente**¹¹ & **Aldo Díaz**¹¹

¹Centre for Neurotechnology and Law (CNL), London, UK.

²International Neurotechnology Governance Observatory (INEGOV), International Center for Neuroscience and Ethics (CINET), Tatiana Foundation, Madrid, Spain. ³CEU Human-Centered Neurotechnology Hub, Universidad Cardenal Herrera-CEU, CEU Universities, Alfara del Patriarca, Spain. ⁴Berkman Klein Center for Internet & Society, Harvard University, Cambridge, MA, USA. ⁵Pontificia Universidad Católica de Chile, Santiago, Chile. ⁶Universidad Externado de Colombia, Bogotá, Colombia. ⁷Universidad de la República, Montevideo, Uruguay.

⁸Universidad Nacional de La Matanza, Buenos Aires, Argentina.

⁹Fundación Kamanau, Buenos Aires, Argentina. ¹⁰Fundación Kamanau, Santiago, Chile. ¹¹Colombara Estrategía Legal, Santiago, Chile.

✉ e-mail: jmmunoz@inecenter.com

Published online: 02 September 2026

References

1. Supreme Court of Chile. Worldcoin ruling (Sentence 35.760-2024) [Anonymized]. *juris.pjud.cl* https://juris.pjud.cl/busqueda/pagina_detalle_sentencia?k=NjBPeUMvQUx6ROJJK2O2Z29kaWtTQT09 (2025).
2. Spanish Data Protection Agency. The agency orders a precautionary measure which prevents Worldcoin from continuing to process personal data in Spain. *aepd.es* <https://www.aepd.es/en/press-and-communication/press-releases/agency-orders-precautionary-measure-which-prevents-worldcoin-from-continuing-to-process-personal-data-in-spain> (2024).
3. Bavarian State Office for Data Protection Supervision. First results of the "Worldcoin" investigation: BayLDA strengthens the rights of data subjects. *lda.bayern.de* https://www.lda.bayern.de/media/pm/pm2024_08_en.pdf (2024).

4. Kindt, E. J. & Fontanillo López, C. A. in *Handbook of Biometric Anti-Spoofing* (eds Marcel, S. et al.) 547–570 https://doi.org/10.1007/978-981-19-5288-3_20 (Springer, 2023).
5. Topcu, B. et al. *EURASIP J. Adv. Signal Process.* **2016**, 100 <https://doi.org/10.1186/s13634-016-0396-1> (2016).
6. Larsson, M. et al. *Biol. Psychol.* **75**, 165–175 <https://doi.org/10.1016/j.biopsycho.2007.01.007> (2007).
7. Kindt, E. *DuD* **31**, 166–170 <https://doi.org/10.1007/s11623-007-0064-6> (2007).
8. Walker, E. M. *Fordham Intell. Prop. Media Ent. L. J.* **XXV**, 831–867 (2015).
9. DeLiema, M. et al. *Innov. Aging* **5**, igab043, <https://doi.org/10.1093/geroni/igab043> (2021).
10. Article 29 Data Protection Working Party. Opinion 3/2012 on developments in biometric technologies (00720/12/EN, WP193). *ec.europa.eu* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (2012).

Competing interests

Å.J., J.M.M., C.A.P., D.B., J.A.I. and J.Á.M. contributed to the drafting of amicus curiae briefs in the case before the Chilean Supreme Court discussed in this Comment. N.M., M.S., C.C., A.d.I.F. and A.D. were members of the legal team representing the claimant in that case.