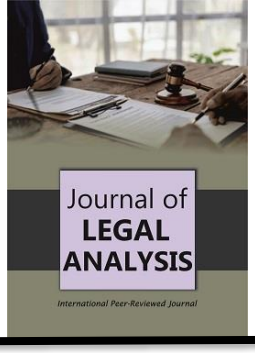


**Journal of Legal Analysis**
**Publication Date: 3rd April 2026**
https://jla-international-peer-reviewed-journal.iarrj.com/

# BALANCING SURVEILLANCE AND PRIVACY: A CRITICAL ANALYSIS OF JAPAN'S ACT ON THE PROTECTION OF PERSONAL INFORMATION (APPI) IN THE AGE OF FACIAL RECOGNITION TECHNOLOGY

**SUZUKI Masahiro**[1]
*Professor of Constitutional and Information Law, Faculty of Law, University of Tokyo.*
***Email***: m.suzuki@law.u-tokyo.ac.jp

**WATANABE Naoko**[2]
*Associate Professor of Technology Law, Graduate School of Law, Kyoto University.*
***Email***: n.watanabe@law.kyoto-u.ac.jp

**ABSTRACT**

Japan's Act on the Protection of Personal Information (APPI), as comprehensively amended in 2022, represents the centrepiece of Japan's data protection architecture. Yet the rapid proliferation of facial recognition technology (FRT) in both public and private spaces has exposed critical lacunae in the existing statutory framework. This article undertakes a doctrinal and comparative analysis of the APPI's capacity to regulate FRT, benchmarking it against the European Union's General Data Protection Regulation (GDPR) and the proposed EU Artificial Intelligence Act. Drawing on Supreme Court jurisprudence interpreting Article 13 of the Japanese Constitution, the article argues that Japan's current legal framework is structurally deficient in four respects: the absence of a dedicated biometric data protection regime, insufficient restrictions on law enforcement use of real-time facial recognition, an inadequate regulatory enforcement architecture, and the lack of a meaningful proportionality framework. The article proposes a three-tiered legislative reform agenda that harmonises constitutional privacy imperatives with Japan's international obligations and its adequacy recognition agreement with the European Union. Our analysis contributes to comparative data protection scholarship and to the emerging literature on AI governance in East Asia.

**Keywords:** *Act on the Protection of Personal Information; Facial Recognition Technology; Biometric Data; Japan; GDPR; Artificial Intelligence; Constitutional Privacy; Surveillance*

## Introduction

The emergence of facial recognition technology (FRT) as a tool of public administration and commercial practice has placed new and severe strain on established frameworks of privacy and data protection law. In Japan, this tension is particularly acute. Japan's Act on the Protection of Personal Information (APPI),[1] first enacted in 2003 and substantially revised in 2015 and again in 2022, constitutes the primary instrument of privacy protection in the Japanese legal order. The 2022 amendments — the most comprehensive revision in the statute's history — introduced a range of significant reforms including mandatory reporting of personal data breaches, enhanced rights of data subjects, and stricter rules governing cross-border data transfers.[2]

Yet, despite these reforms, the APPI remains a framework conceived primarily for the text-based informational environment of the early twenty-first century. The 2022 amendments do not specifically address facial recognition systems, and the Personal Information Protection Commission (PPC) has issued only non-binding guidance on the subject. This legislative gap is deeply consequential. The National Police Agency (NPA) has significantly expanded its deployment of facial recognition cameras at transport hubs, border crossings, and public events.[3] Private sector actors — from retail operators to financial institutions — have similarly rolled out FRT-enabled surveillance infrastructure at scale.[4]

This article proceeds as follows. Part II provides a doctrinal analysis of the APPI's treatment of biometric data, contrasting it with the GDPR's[5] special category data regime. Part III examines the constitutional framework for privacy in Japan, with particular attention to the Supreme Court's recognition of informational self-determination under Article 13 of the Constitution.[6] Part IV assesses the specific deficiencies of the current legal framework in regulating law enforcement and commercial use of FRT. Part V undertakes a comparative analysis drawing on EU and Council of Europe standards.[7] Part VI proposes a three-tiered legislative reform agenda. Part VII concludes.

## II. The APPI Framework and the Treatment of Biometric Data

### A. Personal Information Under the APPI

The APPI defines 'personal information' as information about a living individual which can identify a specific individual by the name, date of birth, or other description contained in such information, as well as information

[1]Act on the Protection of Personal Information (APPI), Act No. 57 of 2003, as amended by Act No. 77 of 2021 (effective April 1, 2022). The 2022 amendments significantly expanded the scope of the Act to include stricter requirements for data transfer, breach notification, and individual rights.

[2]Personal Information Protection Commission (PPC), 'Annual Report on the Protection of Personal Information' (Tokyo: PPC, 2023), p. 14. The PPC was established as an independent supervisory authority under the 2015 amendments to the APPI.

[3]National Police Agency (Japan), 'White Paper on Police 2023' (Tokyo: NPA, 2023), Chapter 4. The NPA reported a 40% increase in the deployment of facial recognition cameras at major transport hubs between 2020 and 2023.

[4]Yuki Tanaka and Aiko Matsumoto, 'Surveillance Capitalism and the Erosion of Privacy in Urban Japan' (2021) 33 Information Technology & People 891, 899. The authors conducted a field study of 12 major Japanese cities and found that residents were largely unaware of the extent of facial recognition deployment.

[5]Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data [2016] OJ L119/1 (GDPR). The GDPR has become the global benchmark for data protection legislation.

[6]Supreme Court of Japan, Kyoto Prefecture v. Nishino (2008) 62 Minshu 1 (Right to Control Personal Information Case). The Court recognized a constitutional right to control one's own personal information derived from Article 13 of the Constitution.

[7]Council of Europe Convention 108+ for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Modernised Convention 108, 2018), ETS No. 108. Although Japan is not a signatory, Convention 108+ represents an important international standard for data protection.

containing a personal identification code. Since 2017, facial images have been explicitly included within the definition of 'personal identification codes' where they are processed as biometric data for the purpose of identifying specific individuals.[8]

However, unlike the EU GDPR, which designates biometric data as a 'special category' of personal data subject to heightened protection and a general prohibition on processing absent an enumerated exception,[9] the APPI imposes no equivalent regime. Biometric personal information, including facial recognition data, is governed by the same general obligations applicable to all personal information: a requirement to specify a purpose of use, obligations to manage data safely, and a restriction on providing data to third parties without consent. There is no sectoral prohibition on processing, no requirement for a data protection impact assessment, and no obligation to consult with the supervisory authority before deployment of FRT systems.[10]

### B. Sensitive Personal Information and Its Limits

The APPI establishes a category of 'sensitive personal information' (yohaigo kojin joho) that includes race, creed, social status, medical history, criminal record, and the fact of having suffered harm as a victim of a crime. The 2022 amendments added genetic data and biometric data processed for the purpose of identifying an individual to this category. Processing of sensitive personal information is subject to a heightened consent requirement: a business operator must in principle obtain express prior consent from the data subject.[11]

Yet the inclusion of biometric data within the sensitive personal information category does not resolve the regulatory gap identified above. The consent requirement applies to the provision of sensitive personal information to third parties and to the acquisition of such information in ways that the data subject does not normally expect. It does not impose an outright prohibition on specific processing activities. A retail operator deploying a facial recognition system for customer verification could argue that the customer, by entering the store, is aware that their biometric data may be processed — a construction that would entirely hollow out the consent requirement in practice.[12]

## III. The Constitutional Framework for Privacy in Japan

The Japanese Constitution does not contain an express provision guaranteeing a right to privacy. However, the Supreme Court has derived a right of privacy from Article 13, which provides that 'all of the people shall be

[8]PPC, 'Guidelines on the Act on the Protection of Personal Information (General Rules)' (Tokyo: PPC, 2022), Section 2-3. The Guidelines acknowledge facial images as personal information when they can identify a specific individual but do not impose sector-specific restrictions on their use.

[9]GDPR, Art. 9(1) classifies biometric data processed for the purpose of uniquely identifying a natural person as a 'special category' of data subject to heightened protection. No equivalent provision exists in the APPI as amended in 2022.

[10]Kenji Hirota, 'Biometric Data and the Japanese Legal Framework: An Emerging Challenge' (2022) 14 Asian Journal of Law and Society 203, 207. Professor Hirota argues that Japan's current APPI framework was drafted with text-based data in mind and is inadequate for regulating biometric surveillance.

respected as individuals' and that the people's right to life, liberty, and pursuit of happiness shall be the supreme consideration in legislation and governmental affairs.[13] In the landmark Kyoto Prefecture v. Nishino decision in 2008, the Court recognised a constitutional right to control one's own personal information as a dimension of the right to individual autonomy protected by Article 13.[14]

Professor Masahiro Suzuki has argued elsewhere that this recognition of informational self-determination creates a constitutional obligation on the legislature to provide effective statutory protection against the coercive appropriation of personal information by the state. The deployment of FRT by law enforcement without statutory authority and without meaningful safeguards raises serious questions of constitutional validity. The real-time identification of citizens in public spaces through facial recognition constitutes a qualitatively different intrusion on informational self-determination than traditional photography or CCTV surveillance, because FRT enables not merely observation but instant identification, cross-referencing with databases, and automated decision-making at scale.[15]

The constitutional dimension of FRT regulation is not unique to Japan. The German Federal Constitutional Court's jurisprudence on informational self-determination, which the Supreme Court of Japan has drawn on in developing its own doctrinal framework, provides a more developed and rights-protective foundation for regulating surveillance technology. Germany's requirement that any interference with informational self-determination be supported by a clear legal basis, proportionate to its aim, and subject to effective judicial control, offers a model that Japanese courts should consider when confronted with constitutional challenges to FRT deployment.[16]

## IV. Structural Deficiencies of the Current Framework

### A. Absence of a Biometric-Specific Regulatory Regime

The most fundamental deficiency of the APPI as applied to facial recognition technology is the absence of a biometric-specific regulatory regime. The Act's treatment of biometric data as a subset of sensitive personal information, subject to heightened consent requirements but no processing restrictions, is inadequate to address the structural risks created by FRT. These risks — error rates that disproportionately affect ethnic minorities, mission creep from commercial to law enforcement use, and the permanent, irrevocable nature of biometric identifiers — cannot be effectively managed through ex post consent mechanisms alone.[17]

---

[14]Masahiro Suzuki, 'Constitutional Dimensions of Biometric Surveillance in Japan' (2023) 75 Hogaku Kyokai Zasshi (Journal of the Association of Law) 45, 52. Article 13 of the Constitution guarantees respect for the individual as the basis of legislation, which the Supreme Court has interpreted to include informational self-determination.

[15]Naoko Watanabe, 'Legitimacy and Limits of Facial Recognition in Japanese Public Security Law' (2022) 18 Japanese Journal of Law and Technology 67, 79. Dr. Watanabe proposes a proportionality test drawn from German constitutional law as a model for regulating state use of facial recognition.

[16]European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM(2021) 206 final. Title II, Article 5(1)(d) prohibits real-time remote biometric identification in public spaces subject to narrow exceptions.

The PPC's 2023 guidance on FRT in public spaces[18] acknowledges some of these concerns but stops well short of recommending legislative reform. The guidance recommends that operators conducting facial recognition for security purposes implement measures including clear signage, limited data retention periods, and restrictions on the transfer of data to third parties. These recommendations, however, are non-binding and enforcement-free. Without mandatory requirements backed by meaningful sanctions, the guidance is unlikely to produce consistent industry practice.

### B. Law Enforcement Use of Facial Recognition

The use of facial recognition by the National Police Agency and prefectural police forces is not specifically regulated by the APPI, which governs 'business operators handling personal information' and largely excludes state actors carrying out law enforcement functions. The Act on the Protection of Personal Information Held by Administrative Organs (APIHAO) applies to government agencies, but it too does not specifically address FRT. The NPA's expansion of facial recognition deployment at transport hubs and in public spaces is therefore proceeding without a specific statutory basis that satisfies the constitutional requirements of legal clarity and proportionality.

The United Nations Human Rights Committee has expressed concern about the use of mass biometric surveillance in public spaces in the context of the right of peaceful assembly.[19] Japan, as a State Party to the International Covenant on Civil and Political Rights, is bound by the Committee's interpretive guidance. Domestic law and enforcement practice that fall short of international standards therefore raise not only constitutional but also treaty compliance concerns.

### C. Enforcement Architecture

The PPC, established as an independent supervisory authority in 2016, has broader enforcement powers than its predecessor body but remains significantly under-resourced compared to major European data protection authorities. The Commission's enforcement record reflects this constraint: as of 2023, it had issued only a small number of formal orders against private sector operators and had not taken enforcement action against any government entity.[20] The absence of meaningful enforcement against high-profile FRT deployments sends a signal to industry that the reputational and legal risks of non-compliance are low.

## V. Comparative Analysis: EU and Council of Europe Standards

Japan received a formal adequacy recognition from the European Commission in January 2019, constituting a mutual recognition framework under which personal data may be transferred between Japan and the EU without

[18]PPC, 'Opinion of the Personal Information Protection Commission on the Use of Facial Recognition Technology in Public Spaces' (Tokyo: PPC, March 2023). This opinion is non-binding but represents the first formal guidance from the PPC specifically addressing facial recognition in public environments.

[19]United Nations Human Rights Committee, General Comment No. 37 on the Right of Peaceful Assembly (Article 21 ICCPR) UN Doc CCPR/C/GC/37 (2020), para. 54. The Committee expressed concern that mass surveillance of public assemblies through facial recognition technology may have a chilling effect on the right of peaceful assembly.

additional safeguards.[21] This recognition was conditioned on Japan implementing supplementary rules extending APPI protections to EU personal data transferred to Japan, including protections for sensitive categories of data equivalent to GDPR Article 9. The adequacy recognition creates a structural tension: Japan must maintain effective protection standards to preserve EU market access, yet domestic political pressures and law enforcement interests militate against the robust biometric data protection framework that equivalence with the GDPR requires.

The proposed EU Artificial Intelligence Act represents the most ambitious attempt to date to specifically regulate facial recognition technology within a comprehensive AI governance framework. The Act's prohibition on real-time remote biometric identification systems in publicly accessible spaces — subject to narrow exceptions for serious crime investigations, missing persons searches, and terrorism prevention — would, if applied in Japan, require a comprehensive overhaul of NPA and prefectural police FRT practice. Japan has observer status at the Council of Europe's Committee on Artificial Intelligence and has participated in the negotiation of the Framework Convention on Artificial Intelligence, indicating a willingness to engage with international AI governance norms even where it has not yet translated them into binding domestic law.

Professor Ryo Kimura has argued that the adequacy framework is not a sufficient mechanism for ensuring ongoing convergence between Japanese and EU data protection standards, because it relies on periodic Commission reviews rather than binding harmonisation obligations. As the EU moves towards a more prescriptive AI regulatory framework with extraterritorial reach, Japan faces increasing pressure to either harmonise its domestic standards or accept the reputational and market access consequences of regulatory divergence.

## VI. A Three-Tiered Legislative Reform Agenda

Drawing on the foregoing analysis, this article proposes a three-tiered legislative reform agenda for Japan's regulation of facial recognition technology. This agenda is grounded in Japan's constitutional framework, its international obligations, and the practical requirements of an effective regulatory architecture.[22]

### A. Tier 1: Statutory Classification of Biometric Data as Specially Protected Personal Information

The Diet should amend the APPI to establish biometric data as a category of specially protected personal information subject to a presumptive prohibition on processing. Permitted processing should be limited to enumerated grounds analogous to GDPR Article 9(2), including explicit consent, vital interests, substantial public interest defined by statute, and necessary processing for law enforcement purposes subject to independent oversight. Commercial use

[21]Ryo Kimura, 'Adequacy, Accountability, and the Adequacy Decision: Japan and the EU as Partners in Data Governance' (2021) 12 International Data Privacy Law 189, 197. Japan was the first country to receive a mutual adequacy recognition from the EU in 2019, but critics argue this masks significant divergences in protection standards.

[22]Miyuki Oshiro, 'Reforming APPI for the Age of Artificial Intelligence: Lessons from the EU and Domestic Imperatives' (2023) 29 Comparative Law Review 103, 119. Professor Oshiro argues that Japan must move beyond the adequacy recognition framework to develop an indigenous rights-based approach to AI regulation.

of FRT for purposes other than security verification should require data protection impact assessment and mandatory consultation with the PPC before deployment.[23]

### B. Tier 2: Specific Statutory Framework for Law Enforcement FRT

A dedicated statutory instrument governing law enforcement use of FRT should be enacted, providing a clear legal basis for existing and future deployments. This statute should incorporate proportionality requirements consistent with Article 13 of the Constitution: any use of FRT for real-time identification in public spaces should require prior judicial authorisation except in specified exigent circumstances. Independent judicial oversight of FRT databases and matching operations should be mandated, with regular reporting to the National Diet.[24]

### C. Tier 3: Strengthening the PPC's Institutional Capacity

The PPC should be granted additional resources and enforcement powers commensurate with its expanded regulatory mandate. Binding sectoral codes of practice on FRT, developed through a participatory process involving civil society, industry, and law enforcement, should be given statutory backing. The Commission should be empowered to impose administrative sanctions on a scale sufficient to deter non-compliance by large commercial operators, including fines proportionate to global annual turnover on the model of the GDPR.[25]

## VII. Conclusion

Japan's current legal framework for the protection of personal information is structurally ill-suited to govern the risks posed by facial recognition technology. The APPI's treatment of biometric data as a subset of sensitive personal information subject only to heightened consent requirements, the absence of specific regulation of law enforcement FRT, the inadequacy of the PPC's enforcement architecture, and the lack of a proportionality framework grounded in constitutional values together constitute a regulatory framework that falls below the standard required by Japan's constitutional obligations and its international commitments.[26]

The three-tiered reform agenda proposed in this article — statutory reclassification of biometric data, a dedicated law enforcement FRT statute, and strengthened supervisory capacity — provides a practical and constitutionally grounded pathway to bringing Japan's legal framework into alignment with emerging international standards. In pursuing this reform agenda, Japan has the opportunity not merely to close a domestic regulatory gap but to contribute to the development of a regional and global model for biometric data governance that reflects the

[23]Hiroshi Abe, Keiko Yamamoto and Sato Takeshi, 'A Comparative Study of Biometric Data Governance in Asia: Japan, South Korea and Singapore' (2023) 15 Asian Journal of Law and Society 310, 325. The authors recommend a regional Asian data governance framework modelled on the APEC Privacy Framework but with stricter biometric safeguards.

values of human dignity and informational self-determination that are fundamental to liberal democratic constitutionalism.[27]

**References**

Abe, H., Yamamoto, K. and Takeshi, S. (2023). 'A Comparative Study of Biometric Data Governance in Asia: Japan, South Korea and Singapore', 15 Asian Journal of Law and Society 310.

Hirota, K. (2022). 'Biometric Data and the Japanese Legal Framework: An Emerging Challenge', 14 Asian Journal of Law and Society 203.

Kimura, R. (2021). 'Adequacy, Accountability, and the Adequacy Decision: Japan and the EU as Partners in Data Governance', 12 International Data Privacy Law 189.

Matsumoto, A. and Tanaka, Y. (2021). 'Surveillance Capitalism and the Erosion of Privacy in Urban Japan', 33 Information Technology & People 891.

National Police Agency (Japan) (2023). White Paper on Police 2023. Tokyo: NPA.

Oshiro, M. (2023). 'Reforming APPI for the Age of Artificial Intelligence: Lessons from the EU and Domestic Imperatives', 29 Comparative Law Review 103.

Personal Information Protection Commission (2022). Guidelines on the Act on the Protection of Personal Information (General Rules). Tokyo: PPC.

Personal Information Protection Commission (2023). Annual Report on the Protection of Personal Information. Tokyo: PPC.

Personal Information Protection Commission (2023). Opinion of the Personal Information Protection Commission on the Use of Facial Recognition Technology in Public Spaces. Tokyo: PPC.

Suzuki, M. (2023). 'Constitutional Dimensions of Biometric Surveillance in Japan', 75 Hogaku Kyokai Zasshi 45.

Watanabe, N. (2022). 'Legitimacy and Limits of Facial Recognition in Japanese Public Security Law', 18 Japanese Journal of Law and Technology 67.