INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

THE INTERNET OF BODIES: RECONCEPTUALISING BODILY AUTONOMY AND PRIVACY IN THE AGE OF BIO-DIGITAL SURVEILLANCE

AUTHORED BY - PRAGATI MISHRA

I. Introduction: where digital networks and human body intertwine

Privacy has been held to be intrinsic to life and personal liberty under article 21 of the constitution, every individual is guaranteed the right to bodily and decisional autonomy without any unreasonable interference. At the same time, digital and technological transformation has led to proliferation of connected health devices- collectively referred to as internet of bodies (IoB)- these continuously generate and transmit physiological data, raising new regulatory challenges. Where statutes such as Digital Personal Data Protection Act,2023 attempts to protect personal data, Information Technology Act,2000 address cyber offences, they fail to address the technologies that interact directly and continuously with the human physiology. Comparative regulatory regimes such as GDPR, Medical Device Regulation and cybersecurity framework by NIST and WHO, underscores the global salience of these issues but also reveal the gaps in addressing cyber-physical harms.

II. Internet of bodies: a distinct technological ecosystem

Generally, there are three identified categories of IOB, as per device's degree of integration-

i. **Wearables**- these include non-medical devices as well as medical devices such as smart watches, personal fitness trackers, for monitoring diabetes, assist in mobility, cardiovascular monitoring, temperature measurement etc. These also include neurotechnological devices for work/learning productivity, augmented and virtual reality devices for entertainment and education, and glasses and helmets in work environments for location tracking, safety monitoring, and job performance enhancement. Combs, razors, toothbrushes, skin care items, mattresses, and other common consumer goods have also included smart sensors which though not affixed to human body, remain in proximity to collect biological and behavioural data

ii. **Invasive**- An internet-connected artificial pancreas that delivers insulin automatically is one example of a smart medical implant. Robotic limbs for movement therapy in

ISSN: 2582-6433

individuals with physical mobility problems. An increasing amount of people have opted to implant chips beneath their skin in recent years, not for medical reasons but rather as a personal decision to expedite daily activities and for convenience—for example, being able to access their homes, offices[1]. People have also tried to improve their bodies with implanted technology as part of the biohacking culture, from small hard drives and wireless routers to magnets and RFID chip implants.

iii. **Others**- While keeping a real-time link to an external machine and the internet, these devices fully integrate with the body.

One of the most prominent businesses in this field is Elon Musk's Neuralink, which is creating "the Link," a brain computer interface, or BCI. Implanted beneath the skull, the coin-sized chip may read brain signals and provide the user control over an external device[2]

The term "Internet of Bodies" (IoB) describes a class of interconnected technologies in which sensors on devices directly interface with human physiological processes, gathering data and, in certain situations, altering bodily function in real time. IoB systems incorporate sensing, communication, and processing layers that continues to collect data, store, observe and even adjust it as per requirement, forecast physical and cognitive functioning, gather biometric data and can even produce algorithmic conclusions that can impact employment evaluations, insurance profiles, medical care and even behavioural nudging, , in contrast to traditional **Internet of Things (IoT)** devices, which mainly collect environmental or behavioural data or traditional medical devices[3]. IoB is situated within larger cyber-physical systems that require strong security guarantees, since the harm by IOB extends beyond the informational or privacy breach to psychological manipulation, emotional distress, physical injury and undermining bodily and decisional autonomy.

[1] Dina Temple-Raston, 'Thousands of Swedes Are Inserting Microchips Under Their Skin' (*NPR*, 22 October 2018) https://www.npr.org/2018/10/22/658808705/thousands-of-swedes-are-inserting-microchips-under-their-skin accessed 7 December 2025.

[2] Arjun Kharpal, 'The Next Generation of the "Internet of Bodies" Could Meld Tech and Human Bodies Together' (*CNBC*, 1 June 2024) https://www.cnbc.com/2024/06/01/internet-of-bodies-could-meld-tech-and-human-bodies-together.html?msockid=25f4d6b8c1e16c4a0534c61fc5e16ed6 accessed 5 December 2025

[3] Dr Deepa A and V N Aswin Kumar, 'A Study on Internet of Behaviors (IoB)' (2022) *International Journal of Novel Research and Development* 7(5) 1182 https://www.ijnrd.org/papers/IJNRD2205157.pdf accessed 30 November 2025

ISSN: 2582-6433

III. From Consent to Constitution: Addressing Legal Gaps in The Internet of Bodies

i. The current legal regime treats IOB either a part of data protection law, which focuses on information and privacy breaches or through medical regulations, which address physical safety and not data exploitation. A legal vacuum is hence created whereby bio-digital harms remain insufficiently governed. Treating IOB as a part of personal data undermines in nature and unique vulnerability of the individuals, IoB systems can directly impact insulin supply, brain stimulation, heart rhythms, and behavioural modulation, none of these issues are well addressed by privacy-based safeguards.

ii. The principle of informed consent which forms the bedrock of data laws does not work with IOB since data collection is continuous and adaptive which might even evolve in the future. This makes the consent given during initial agreement totally irrelevant thereby reducing the principle to a mere formality[4].

iii. Since the data protection laws deal primarily with data, they effectively fail to regulate the inferential analytics, leaving the sensitive conclusions related to disease susceptibility, emotional states, productivity, or cognitive decline out of its purview. This leads to discriminatory or coercive decision making without direct access to identifiable personal data.

iv. Current regulations ignore the degree of bodily intrusion present in IOBs thereby treating low risk wearable at par with high risk implantable or neural device for compliance obligations and ignore the risk proportionality associated by treating them like medical or environmental regulation.

v. Cross-border data transmission methods are still inappropriate for bio-digital infrastructures, as cloud-based analytics could be contracted out to countries which lack human rights or health regulations, resulting in regulatory arbitrage and enforcement gaps for global IoB service provider.

vi. The legal system fails to give legal recognition to data induced bodily harm, the data laws address information or privacy breach whereas hardware malfunctions are covered under contracts thereby leaving IOB software update, IOB confusion, algorithmic optimisation and third part analytics out of the scope of legal framework.[5]

[4] Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880.
[5] Andrea M Matwyshyn, 'The Internet of Bodies' (2020) 61 *William and Mary Law Review* 77.

ISSN: 2582-6433

vii. The gaps throw a light upon the urgency of having a legal architecture that covers bio-technical information thereby evolving the individual data rights into integrated bodily governance mechanisms capable of handling cyber-physical vulnerability in an era of technology.

viii. The landmark case of **Justice KS Puttaswamy vs. UOI**[6] established the strongest foundation for IoB regulation. The court clearly held that right to privacy includes bodily privacy as well as informational privacy as a part of Article 21 thereby making bodily autonomy, integrity, and privacy an inviolable principle of law. The sacrosanct zone of bodily autonomy and integrity is per se perforated when the IoB devices harvest biological data or control heartbeat or cognitive actions. This creates a dichotomy when even though the user has surgically placed physical hardware, the "right to function" is still tethered to the manufacturer's corporate solvency. Any EULAA (end user license agreement) which allows the company to unilaterally disable, control, access an implant without a clear, proportional law violates the "reasonableness test" as established in puttaswamy.

ix. In the case of **Common Cause vs UOI 2018**[7] supreme court affirmed the right to bodily autonomy and to refuse medical treatment as a part of right to die with dignity under Article 21. The right to refuse does not include "the right to software autonomy." An update or a model that interferes with natural functioning transforming our biological self into a licensed commodity must also be unconstitutional.

x. **Selvi vs State of Karnataka**[8] expanded the scope of Article 20(3) beyond mere verbal testimony to include "mental privacy". IoB, which involuntarily collect biological and cognitive data should also fall under "testimonial compulsion" since the state and corporation cannot forcibly extract the mental information.

xi. Currently, software is treated as a medical device under **Drug and Cosmetics Act**[9] and **Medical Device Rules, 2017**[10]. An implant is treated as a drug however these rules fail to account for the "Continuity of service." A failed drug is a one-time incident but a failed implant is a continuous body trespass. further an insolvency in case of an IoB can effectively evict the user digitally from their own prosthetic or organ.

[6] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.
[7] *Common Cause v Union of India* (2018) 5 SCC 1.
[8] *Selvi v State of Karnataka* (2010) 7 SCC 263.
[9] Drugs and Cosmetics Act 1940 (India).
[10] Medical Devices Rules 2017 (India).

ISSN: 2582-6433

xii. BNS requires some sort of physical contact involved in criminal force, and IT law require some sort of cybercrime. However, IoB are capable of harming without any contact e.g. what if a pacemaker is remotely accessed to induce arrhythmia, the laws are yet not clear if this situation would be covered by current laws or is a whole new form of crime.

IV. INTERNATIONAL FRAMEWORKS AND IOB CHALLENGE

i. GENERAL DATA PROTECTION REGULATION

The regulation classifies the biometric and health data as a special category data under article 9. It also requires certain safeguards such as lawful basis, purpose limitation, data minimisation etc. however, GDPR has been inadequate to deal with IOB since the focus of the regulation is informational privacy rather than physical or neurological integrity. The regulation is silent upon a consent which is continuous and automated hence reducing the consent requirements in case if IOB to a mere formality, the inferred health and behavioural traits are outside the scope of protected data, the regulation further fails to protect the cases of harmful software updates of device malfunctions[11].

ii. HIPAA

The law protects the medical records held by healthcare professionals and insurers yet it is not enough since the AI driven medical conclusions and predictions fall largely outside the scope of HIPAA, the secondary usage of bodily data is permitted and devices like fitness tracker, neural headsets and workplace monitors are not covered within the law[12]

iii. OECD PRIVACY GUIDELINES AND CROSS BORDER TRANSFER REGIMES

These allow the free flow of data with privacy safeguards yet they are structurally incapable of dealing with IOB because they are designed in a way to regulate and facilitate trade rather than protect bodily autonomy. They govern data handling and not physical consequences and it lacks binding enforcement mechanisms[13].

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.
[12] Health Insurance Portability and Accountability Act 1996, Pub L No 104-191, 110 Stat 1936 (US).
[13] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Enhancing Access to and Sharing of Data* (OECD, C(2019)137, 2019) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0441 accessed 7 December 2025.

ISSN: 2582-6433

iv. ICCPR, ICESCR

They protect privacy, dignity, health, and autonomy yet they are insufficient because their primary focus is state action hence, they have a limited reach over private technology corporations, the rights guaranteed are abstract rather than technologically specific. Further, no direct remedy is provided for cross border IOB harm[14].

v. INTERNATIONAL HEALTH LAW AND BIOMEDICAL ETHICS INSTRUMENTS

These rely on key instruments such as cioms/who guidelines and UNESCO'S declaration on bioethics. These are limited to medical contexts and do not cover IoB, there are no rules which deal with continuous biological monitoring. they are silent on cloud analytics and AI inferences.

vi. UDHR

It protects "freedom of thought" and assumes that the mind is impenetrable fortress however, IoB allows continuous "mental surveillance" that currently does not violate the existing treaties[15].

V. SAFEGUARDING SELF: LEGAL, GOVERNANCE AND POLICY RECOMMENDATION FOR IoB

i. IoB collects information directly from the interaction with the human body, such information includes biometric, neurological, behavioural, physiological signals, any harm to such data can directly cause physical injury, emotional distress, and loss of decisional autonomy. IoB implicates constitutional and human rights issues therefore, it requires a separate legal recognition as a distinct category of protected interest. Without heightened legal standards, regulatory frameworks will continue to remain misaligned with the bio-digital harms.

ii. The regulation of IoB must be proportionate to the risk associated and the degree of bodily intrusion. A risk-tier classification would enable regulators to impose a stricter licensing, monitoring and security requirements thereby preventing high risk technologies escape the legal scrutiny[16].

[14] International Covenant on Civil and Political Rights, 999 UNTS 171 (opened for signature 16 December 1966, entered into force 23 March 1976).
[15] Universal Declaration of Human Rights GA Res 217A (III), UN GAOR, 3rd Sess, UN Doc A/810 (10 December 1948).
[16] Andrea M Matwyshyn (ed), *Consumer Protection and the Internet of Bodies* (Cambridge University Press 2022).

ISSN: 2582-6433

iii. Governance should typically focus more on preventive oversight model rather than a liability model by mandatory imposition of Biological Impact Assessment[17]. The assessment must evaluate not only data protection but also the behavioural, physical, psychological, neurological impacts of continuous monitoring and algorithms. Such assessment becomes more important in the cases where the data collected impacts the behavioural patterns directly.

iv. Since one time consent reduces to a mere formality in cases of IoB, legal frameworks should therefore mandatorily require periodic renewal of consent, approval for updates and withdrawal of consent should be an effective and easier process. This would make consent a genuine expression of self determination rather than a mere formality legitimising bodily surveillance.

v. Rule of procedural fairness and substantive equality must be inculcated by allowing right to explanation, review and contesting the inferences and analysis drawn by continuous data collection. Lack of legal recognition to inferred results leads to discriminatory and coercive practices in cases where such information affects legal or economic opportunities such as employment or insurance pricing.

vi. Cross- border transfer of such high-risk bodily data must be subjected to strict scrutiny and enhanced safeguards that reflect the sensitivity and irreversibility associated with the biological harms[18]. Mandatory data encryption, data localisation and offshore data analytics should be required for the high-risk data categories to ensure retention of remedial access and regulatory oversight with the individuals.

vii. Strict and joint liability regime must be adopted to ensure that the victims do not lose the right to compensation due to technical complexity or fragmentation of contractual liabilities thereby ensuring deterrence and corporate accountability of manufacturer, developer, service provider, and analytics platform, which are jointly responsible for shaping bodily outcomes.

viii. Mandatory audits, transparency obligations, and reporting of adverse incidents thereby shifting the framework from complaint driven into preventive supervision to ensure enhanced accountability and early detection of risks must be implemented.

ix. International cooperation of multinationals operating in IoB is also essential to prevent regulatory breaches. Harmonisation of benchmarks for data security, device safety and

[17] Nuffield Council on Bioethics, *Bioethics and Data-Driven Health Care* (2015) https://www.nuffieldbioethics.org/publications accessed 7 December 2025

[18] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD Legal Instruments, C(2019) 65, 2019) https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 accessed 7 December 2025.

ISSN: 2582-6433

accountability must be mandated to promote rights protection and facilitate responsible innovation.

x. State must be made obliged to regulate private technological power affecting the bodily autonomy. Constitutional jurisprudence of IoB must ensure protection against foreseeable private harms. Failure to regulate bio-technical ecosystem that regulates continuous bodily surveillance and behavioural monitoring must necessarily constitute constitutional neglect rather than mere regulatory breach. Legislative intervention is therefore the primary requirement in this domain.

VI. CONCLUSION

The interplay of relationship between the individuals, technology and governance has transformed the digital infrastructure from merely observing human activities to controlling, mediating and regulation bodily and cognitive functions. The article has examined how the risks associated with the IoB and bio-digital ecosystem are far more dangerous than a data or a privacy breach and how the current sector specific laws are incapable of addressing the legal issues linked to the continuous evolving nature of IoB. The inadequacy of consent framework, fragmentation of authorities, absence of liability models creates a legal vacuum resulting in the violation of autonomy, dignity, and privacy as well as security. In this light the article examines the nature of IoB beyond privacy centric approach to something that violates the constitutional and human rights thereby requiring the re-consideration of the limitations of fundamental rights and transforming the current compliance based reactive legal framework into precautionary, rights-based framework that comes into play before the deployment of these technologies into the market.

Ultimately, the challenge posed by the IoB is not simply how to regulate another category of emerging technology but how to preserve the constitutional democracy when the biological life itself becomes programmable and economically exploitable. The legal framework therefore requires the transition from protecting the data as a mere informational commodity to protecting the human within the socio-technical system. Without such a shift the regulatory framework will justify the bio-digital governance that is efficient, profitable, and technologically driven yet fundamentally incompatible with the core constitutional principles and the rule of law.