

INTERNET OF BODIES AND PRIVACY ISSUES

Sinisa S. Domazet¹

¹Metropolitan University, Tadeusa Kosciuska 63, Belgrade, Republic of Serbia,
sdomazetns@gmail.com, ORCID ID [0000-0002-5964-2249](https://orcid.org/0000-0002-5964-2249)

Digital Object Identifier (DOI): [10.70995/JYNI7237](https://doi.org/10.70995/JYNI7237)

Article Category: Scientific paper

Article Type: Review paper

Received: 29th July 2025

Accepted: 7th August 2025

Abstract: *The rapid development of modern information and communication technologies as well as artificial intelligence has penetrated into all aspects of human life and modern society. This led to the emergence of the Internet of Things, but also to a new technological breakthrough in the form of the Internet of Bodies (IoB). The term “Internet of Bodies” was coined for the first time by Andrea Matwyshyn, labeling it as “a network of human bodies whose integrity and functionality rely at least in part on the Internet and related technologies, such as artificial intelligence”. The goal of the research in the paper is to analyze the relationship between the obligation to protect personal data and the Internet of Bodies, while pointing out the problems of misuse of data that have arisen through the use of modern technologies. Normative method and legal-logical methods of induction and deduction were used in the paper.*

Keywords: Law, Privacy, Internet of Bodies, Security

1. INTRODUCTION

The rapid development of modern information and communication technologies as well as artificial intelligence has penetrated into all aspects of human life and modern society. This led to the emergence of the Internet of Things, but also to a new technological breakthrough in the form of the Internet of Bodies (IoB). This development includes an expanding array of devices that combine software, hardware, and communication capabilities to track personal health data, provide vital medical treatment, or enhance bodily comfort, function, health, or well-being (Lee, et al., 2020). The term “Internet of Bodies” was coined in 2016 by American Professor, Andrea Matwyshyn, who describes it as “a network of human bodies whose integrity and functionality rely, at least in part, on the internet and related technologies.” (Anon., 2025).

According to Matwyshyn, the Internet of Bodies might be divided into three generations of technologies—body external, body internal, and body melded. First-generation IoB medical devices include devices such as Internet-enabled robotic surgery machines and connected prosthetics that a patient operates from a mobile phone. Second-generation IoB technologies refer to those IoB devices where a portion of the device resides inside the body or accesses the body by breaking the skin. Third-generation IoB devices meld the human mind with external computers and the Internet (Matwyshyn, 2019). In the near future, a connected body might even become a platform capable of transmitting and receiving data from other human bodies (e.g., brain-to-brain interfaces) (Stefanaki, 2025).

The Internet of Bodies has undoubtedly introduced numerous innovations in the functioning of modern human life, particularly in the field of healthcare. However, it has also brought with it many challenges related to the protection of personal data, consumer rights, intellectual

property rights, the possibility of hacking and cyberattacks, issues with interoperability, ethical concerns, and more. In short, it can be argued that the Internet of Things (IoT) and the Internet of Bodies (IoB) essentially share the same risks and concerns.

The goal of the research in this paper is to analyze the relationship between the obligation to protect personal data and the Internet of Bodies, while highlighting the problems related to data misuse that have emerged through the use of modern technologies. First, statistical data regarding the Internet of Bodies will be analyzed, followed by a focus on the analysis of challenges arising from these technologies in relation to personal data protection, based on real-world examples.

2. STATISTICAL DATA REGARDING THE INTERNET OF BODIES

The Internet of Bodies is constantly growing, as evidenced by numerous statistics from various sources (Demandsage, Statista, IoT Analytics, FinleyUSA, European Commission), which show that the number of connected IoB devices is growing year by year and further growth is expected in the future.

Undoubtedly, the most popular IoB devices are those that are not embedded in the human body—that is, those that remain outside the human body (such as smartwatches and Bluetooth-connected breast pumps). When it comes to the use of smartwatches, as of 2025, there are 454.69 million smartwatch users worldwide, marking a 41% increase from the 323.99 million users in 2023. Looking ahead, the number of smartwatch users is expected to continue rising, reaching an estimated 740.53 million by 2029. Apple holds 21% of the global smartwatch market share. Huawei follows with a 14% share, while Samsung accounts for 11% of the market, others 54% (Kumar, 2025). The global smartwatch market is set to reach \$143.19 billion by 2032. The market is predicted to grow at a CAGR of 15.6% between 2024 and 2032. 92% Of People Use Smartwatches To Maintain Their Health And Fitness 88% of the people reported that smartwatches helped them achieve their fitness goals. Besides, almost 1 in 2 smartwatch users used smartwatches to exercise regularly (Kumar, 2025).

According to the latest available data, there are approximately 14.76 billion connected IoT devices. The number of current IoT devices (14 billion) may seem staggering. But thanks 5G and other technologies, this figure is expected to grow almost 2x to 25.44 billion total IoT devices by 2030. There has been a notable shift from non-IoT devices to IoT devices over the last decade. In fact, by 2030, 75% of all devices are forecast to be IoT. The number of IoT platforms has increased year-over-year. In 2015, there were 260 publicly known IoT platforms. This figure jumped to 360 in 2016. And increased by a further 90 to 450 the following year. By 2019 there were 620 publicly known IoT platforms - 426 of which were still active in 2021 including global names like Microsoft and Amazon. In 2020, IoT spending reached \$749 billion. In 2022, global IoT spending was predicted to hit \$1 trillion. And in 2023, predicted spending rose to \$1.1 trillion, continuing the increased rate of growth year-over-year. Despite a marked increase in IoT spending in recent years, market share by region isn't expected to change drastically. Back in 2018, the Asia Pacific region had the largest regional market share with 37% (over a third of total global IoT spending) (Howarth, 2024).

Although the Internet of Bodies is a narrower concept than general healthcare IoT, most health-related smart implants, wearables, and ingestibles fall under Healthcare Internet of Things (IoT). Healthcare IoT global revenue is projected to be around USD 93.28 billion in 2025, up approximately 11.3% year-on-year (Anon., 2024).

Based on the above data, a global growth of the Internet of Bodies can clearly be observed, which is a logical consequence of the worldwide expansion in the use of IoT.

3. LEGAL CHALLENGES OF IoB IN RELATION TO THE RIGHT TO PRIVACY

The Internet of Bodies is undoubtedly very useful in everyday human life, especially in the field of healthcare, but these technologies also carry certain risks to privacy, particularly concerning public health. Privacy risks include: a) the possibility of unauthorized access to biometric and health data, i.e., hacking of medical devices, which would expose the most sensitive personal and health-related information; b) redesigning devices originally made for medical purposes into devices that could be used for mass (non-selective) surveillance without the consent of the users, enabling direct control over their behavior; c) misuse of biometric and health data for discrimination in the workplace or other situations; d) misuse of data to create profiles of personal data subjects; e) insufficient information and often limited knowledge of health device users regarding giving consent for the collection and processing of personal data, especially if the data processing is automated.

Regarding legal regulations related to the Internet of Bodies, there is no universal legal framework in this area; instead, IoB is indirectly regulated by several legal acts worldwide, primarily in the USA and the European Union.

Concerning the European Union, we should mention Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance), further: CRA. This act is of exceptional importance for IoB, as it stipulates that IoT devices (and therefore IoB devices) must be made to ensure a high level of cybersecurity, especially regarding the protection of personal body-related data.

Secondly, manufacturers are obliged to notify the EU agency for cybersecurity (ENISA) of any exploited product vulnerability or incident within 24 hours of becoming aware of the vulnerability or incident. This is very important because IoB devices can significantly affect citizens' health (for example, pacemakers).

Thirdly, the manufacturer is obliged to provide effective support for at least 5 years for vulnerabilities during the life cycle of the product with digital elements, or during the expected life of the product, whichever is shorter.

Fourthly, Annex I of this act contains provisions that are of particular importance for the protection of personal data, which can also apply to IoB. In this regard, products with digital elements must (if applicable), among other things: ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems; protect the confidentiality of stored, transmitted, or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms; protect the integrity of stored, transmitted, or otherwise processed data, personal or other, commands, programs, and configuration against any manipulation or modification not authorized by the user, as well as report on corruptions; process only data, personal or other, that are adequate, relevant, and limited to what is necessary in relation to the intended use of the product ('data minimization'); protect the availability of essential functions, including resilience against and mitigation of denial of service attacks; minimize their own negative impact on the availability of services provided by other devices or networks; be designed, developed, and produced to limit attack surfaces, including external interfaces; be designed, developed, and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques; provide security-related information by recording and/or monitoring relevant internal activity, including access to or

modification of data, services, or functions; ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users (European Union, 2022).

It is also important to note that IoB devices such as pacemakers and ingestible sensors, which are regulated by specific medical device regulations, are exempt from the application of this act. On the other hand, consumer devices (for example, smartwatches, fitness wearables) fall under the CRA and must meet cybersecurity design and update requirements.

Regarding specific cases of IoB's impact on privacy, it is interesting to mention the Pacemaker Hacking case. In 2017, nearly 500,000 pacemakers were recalled due to cybersecurity vulnerabilities, highlighting the growing threat of hacking in life-sustaining medical devices. Although no patient harm was reported, the FDA confirmed that attackers could potentially access the devices remotely, drain their batteries, or cause them to deliver inappropriate shocks. This raised serious privacy and safety concerns, as software-related risks introduced a new dimension of danger for implantable devices. Updating the firmware required in-person procedures and carried its own risks, since any malfunction during the update could be life-threatening. Most physicians and patients—especially those dependent on pacemakers—chose not to update the firmware due to the lack of clear data on potential consequences. Experts emphasized that cybersecurity must be built into the entire lifecycle of medical devices, from design to real-world use. As internet-connected implants become more common, future risks to patient privacy and security are likely to increase. Patients enjoy the convenience of remote monitoring and data access, but they must also take responsibility for keeping their devices secure through regular updates. Because technology and cybersecurity threats evolve rapidly, devices with multi-year lifespans must be adaptable and continuously protected. Ultimately, maintaining trust in these deeply personal medical technologies requires absolute assurance of data safety and protection from exploitation (Kuehn, 2018).

Also noteworthy is the example of the Fitbit and Google acquisition from 2019. Google's acquisition of Fitbit (a wearable device that tracks personal metrics, including exercise, calories, weight, sleep habits, and much more) in November 2019 raised serious concerns about user privacy, despite official assurances. Although Google promised not to use Fitbit's health and wellness data for advertising, experts warned that other forms of personal data could still be exploited. Fitbit collects a vast array of sensitive information, including names, emails, birthdates, health metrics, sleep patterns, and even geolocation history. Critics pointed out that combining this data with Google's existing information — such as search history and emails — could result in a disturbingly complete profile of an individual. This level of surveillance introduces significant risks, including potential misuse by employers, insurers, or financial institutions. Privacy advocates expressed doubt that current promises not to use the data for advertising would remain unchanged in the future. The possibility that health data could affect job prospects, credit approval, or insurance access highlights the far-reaching consequences. Some users chose to abandon Fitbit devices altogether, fearing irreversible privacy intrusions. While users can delete their accounts, the process takes time, and by then, much of the data might have already been analyzed or shared. Ultimately, the situation underscores the urgent need for stronger data protection standards and greater transparency from tech giants (Anon., 2024).

One of the most recent cases concerns the incident on June 3, 2024, when NHS England confirmed that patient data managed by pathology testing organization Synnovis was stolen in a ransomware attack. The Russian cybercriminal group Qilin claimed responsibility and shared nearly 400GB of private information on the dark web to pressure Synnovis for ransom. NHS England stated there is no evidence that test results have been published, but investigations are

still ongoing. Over 3,000 hospital and GP appointments were disrupted due to the attack. Patients were advised to attend appointments as scheduled unless told otherwise and to seek urgent care as usual. A sample of stolen data included patient names, birthdates, NHS numbers, and blood test descriptions, which cybersecurity experts described as one of the most harmful cyberattacks in UK history. Additionally, business account spreadsheets detailing financial arrangements were stolen. The attackers infiltrated Synnovis's computer systems, encrypted critical data, and made IT systems unusable. They also downloaded private data to further extort Synnovis for ransom payment in Bitcoin, but it remains unknown if a ransom was paid. The attackers claimed they targeted Synnovis to punish the UK for insufficient support in an unspecified war, and NHS England is working with law enforcement and Synnovis while providing support to affected patients (Casey, 2024). This example clearly highlights the dangers arising from IoB and digital diagnostics, further emphasizing the importance of the CRA.

4. CONCLUSION

The rapid development of the Internet of Bodies (IoB) concept represents a transformation in how personal and health data are collected, transmitted, and analyzed. However, this transformation carries serious risks to privacy and cybersecurity that remain inadequately addressed. As demonstrated by the 2024 ransomware attack on Synnovis, in which hackers stole and leaked sensitive patient data from the UK's NHS system, the vulnerability of healthcare infrastructure to cyber threats has serious consequences. Similarly, Google's acquisition of Fitbit continues to raise concerns about the merging of biometric and behavioral data for commercial profiling. Earlier, the 2017 pacemaker recall case showed that compromised IoB devices can directly threaten human lives.

These examples point to several systemic issues. First, there is a lack of comprehensive international regulation to address these challenges. Second, real-world cases (which are increasing in number) reveal a low level of cybersecurity in IoB devices, particularly in healthcare and consumer sectors. Third, transparency is lacking, and users are insufficiently informed during incidents. Fourth, there is unclear accountability among device manufacturers, service providers, and data platforms.

Undoubtedly, the EU Cyber Resilience Act (CRA) provides a good starting point, as it requires digital product manufacturers—including those producing IoB devices—to implement security measures by design and to report serious incidents. However, its implementation must be consistent across the European Union. Moreover, technical protection must be significantly improved, which includes regular software updates, strong encryption, authentication, and secure firmware. Organizational measures should not be overlooked either; high-tech companies and healthcare providers must conduct serious risk assessments, allocate financial resources for monitoring systems, and establish incident response plans. Failure to do so—or delayed reporting, as in the Synnovis case—can severely undermine public trust.

Continuous user education about the risks associated with IoB devices is also necessary, enabling consumers to make informed decisions about their purchase and use. This especially applies to transparency regarding the collection, processing, and sharing of personal data, where user consent must be clear and unambiguous. Since cyberattacks are often carried out by organized criminal groups (such as Qilin and many others worldwide), global international cooperation between East and West is essential to mitigate or eliminate cyber threats.

There is no doubt that IoB can significantly contribute to more effective and personalized healthcare. However, the issue of protecting users' privacy and security remains unresolved and must be addressed through legal, technical, organizational, and ethical mechanisms. The

analyzed cases clearly show that we are facing a systemic threat that demands continuous, interdisciplinary attention and global cooperation—regardless of geopolitical divisions between the world’s major powers. In this way, public trust, which has been seriously damaged by increasing privacy violations through IoB devices, could be restored and digital inequality prevented from deepening.

BIBLIOGRAPHY

Anon., 2024. *A World of Hurt? — Is Google’s Purchase of Fitbit a Data Privacy Risk?*. [Online] Available at: <https://www.spirion.com/blog/google-fitbit-acquisition-data-privacy-risk> [Accessed 26 July 2025].

Anon., 2024. *Healthcare IoT - Worldwide*. [Online] Available at: https://www.statista.com/outlook/tmo/internet-of-things/healthcare-iot/worldwide?utm_source=chatgpt.com [Accessed 23 July 2025].

Anon., 2025. *Governing Data in the Age of the Internet of Bodies*. [Online] Available at: <https://telecomreview.com/articles/reports-and-coverage/8964-governing-data-in-the-age-of-the-internet-of-bodies/> [Accessed 23 July 2025].

Casey, I., 2024. *NHS confirms patient data stolen in cyber attack*. [Online] Available at: <https://www.bbc.com/news/articles/c9777v4m8zdo> [Accessed 26 July 2025].

Kuehn, B., 2018. *Pacemaker Recall Highlights Security Concerns for Implantable Devices*. [Online] Available at: <https://www.ahajournals.org/doi/10.1161/CIRCULATIONAHA.118.037331> [Accessed 26 July 2025].

Kumar, N., 2025. *Smartwatch Statistics 202: Market Shares & Sales Data*. [Online] Available at: <https://www.demandsage.com/smartwatch-statistics/> [Accessed 23 July 2025].

Lee, M. et al., 2020. *The Internet of Bodies - Opportunities, Risks, and Governance*. [Online] Available at: https://www.rand.org/pubs/research_reports/RR3226.html [Accessed 23 July 2025].

Matwyshyn, A. M., 2019. The Internet of Bodies. *William & Mary Law Review*, 61(1), pp. 77-167.

Stefanaki, E., 2025. *The Internet Of Bodies: Connectivity Enhancing Humans*. [Online] Available at: <https://lesi.org/article-of-the-month/the-internet-of-bodies-connectivity-enhancing-humans/> [Accessed 22 July 2025].