Int J Ethics Soc 2024; 6(3): 64-66

10.22034/ijethics.6.3.64

INTERNATIONAL JOURNAL OF Ethics & Society

Letter to Editor

Ethical Challenges of Using the Internet of Behavior in the Medical and Healthcare Practice

Zahra Sadeqi-Arani*, Esmaeil Mazroui Nasrabadi

Department of Management and Entrepreneurship, Faculty of Financial Science, Management and Entrepreneurship, University of Kashan, Kashan, Iran.

Corresponding Author: Zahra Sadeqi-Arani, Department of Management and Entrepreneurship, Faculty of Financial Science, Management and Entrepreneurship, University of Kashan, Kashan, Iran. E-mail: sadeqiarani@kashanu.ac.ir

Received 08 Aug 2024 **Accepted** 20 Aug 2024 **Online Published** 02 Nov 2024

How to Cite: Zahra Sadeqi-Arani*, Esmaeil Mazroui Nasrabadi. Ethical challenges of using the internet of behavior in the medical and healthcare practice, Int J Ethics Soc. 2024;6(3): 64-66. doi: 10.22034/ijethics.6.3.64

[DOI: 10.22034/ijethics.6.3.64]

The Internet of Behavior (IoB), an advanced evolution of the Internet of Things (IoT), has emerged as a significant technological innovation in the past decade. IoB aims to identify specific behavioral patterns by collecting and analyzing individuals' behavioral data, ultimately enhancing decision-making processes and improving service provision [1]. This technology integrates technological innovation, data analysis, and behavioral sciences, utilizing diverse sources such as wearable smart devices, ingestible and injectable technologies (including health bracelets, smartwatches, and sensors), social media, and other digital tools connected to the body, to gather data [2, 3]. By incorporating three distinct domains, human social space, physical space, and cyberspace, IoB seeks to create a comprehensive informational framework designed to predict and modify behaviors [4].

One of the most significant applications of IoB is in the medical and health sector [5]. Through data collection from wearable devices such as health bracelets and smartwatches, IoB can provide valuable insights into patients' physical and behavioral conditions [6]. This information includes data on physical activity, sleep patterns, heart rate, and other vital signs, which can assist healthcare professionals in achieving more accurate diagnoses and better managing patients' health. For instance, data obtained from wearable devices can identify risk factors and inform preventive treatment measures [7]. Monitoring physical activity and sleep patterns, for example, can aid in the prevention of cardiovascular diseases. Additionally, ingestible digital pills containing IoT sensors, encapsulated with standard medications, enable reliable monitoring of medication adherence [8]. Furthermore, the continuous monitoring and behavioral data analysis facilitated by wearable devices can support the provision of personalized treatments. By analyzing the dietary habits and daily activities of diabetic patients, healthcare providers can offer treatment plans better aligned with patients' lifestyles [9]. Moreover, IoB devices allow for the continuous collection of real-time data from patients, offering immediate support in the event

of complications. This is particularly beneficial for chronic patients and the elderly, as it facilitates remote monitoring and healthcare services [10].

Despite the many benefits IoB offers the medical and health sector and its potential to improve healthcare services, the deployment of this technology raises significant ethical challenges. These challenges include:

Privacy:

The collection of behavioral data inherently risks violating individual privacy. Wearable devices that monitor patients' daily activities, geographic locations, and dietary habits can expose highly personal and sensitive information. There is a tangible risk that this data could be sold or shared without the user's consent [5, 11]. A notable example is the Fitbit scandal, where user data was sold to insurance companies without user consent. Fitbit products, which monitor users' physical activities, including steps taken per day, heart rate, sleep quality, and stairs climbed, illustrate the potential for privacy breaches.

Data Security:

The behavioral data collected by IoB systems must be securely stored and transmitted. A case in point is the cyberattack on the Synovus Pathology Service Center in the UK, where sensitive patient information was stolen and exposed by hackers [9]. Such incidents underscore the critical need for robust security measures in handling IoB data.

Transparency:

A significant ethical concern associated with IoB is the lack of transparency in data collection and usage. Users must be fully informed about how their data is collected, processed, and utilized. Obtaining informed consent for collecting and using behavioral data presents a challenge [12]. Companies and organizations leveraging IoB technology must clearly communicate to patients the types of data being collected and its intended uses when seeking consent. For instance, if an insurance company intends to use behavioral data to determine premiums, this must be explicitly disclosed to patients [6].

Behavioral Manipulation:

The capacity of IoB to analyze and influence patient behavior raises concerns about potential manipulation. For example, behavioral data collected by a health program could be exploited for commercial purposes, such as targeted advertising. A particularly concerning example is the use of behavioral data by pharmaceutical companies to promote specific products to patients. This secondary use of data and the potential for behavioral manipulation may undermine patient autonomy, leading to conflicts of interest where commercial considerations supersede patients' health interests [9].

Equality in Access:

Socioeconomic disparities can exacerbate inequality in access to IoB technologies. For example, patients from disadvantaged communities may lack access to wearable devices and related services, thereby worsening healthcare inequalities [13, 14].

Psychological and Social Impacts:

The pervasive use of IoB technology can have unintended psychological effects on patients. Continuous monitoring and data collection can foster a sense of constant surveillance, contributing to increased anxiety and stress. Additionally, over-reliance on monitoring technologies might reduce human interactions in healthcare, potentially leading to feelings of loneliness and isolation among patients [11].

Identifying these ethical challenges and addressing them proactively in the deployment of IoB technologies is crucial to maximizing the benefits of this technology. The application of monitoring technologies like IoB must not compromise patients' human dignity or instill a sense of diminished independence, control, and privacy. Furthermore, while employing

[DOI: 10.22034/ijethics.6.3.64]

algorithms and automated systems to analyze IoB data, the role of human oversight and decision-making should not be diminished. Patients should always have the opportunity to consult with their healthcare providers and be active participants in decisions concerning their health. Developing ethical protocols, including stringent security standards, informed consent processes, and the protection of patients' rights to access and control their data, while ensuring that this data is not exploited for advertising or commercial purposes, can enhance users' willingness to engage with IoB technologies. Healthcare organizations must assume full responsibility for safeguarding patient data and be held accountable in the event of security breaches or data misuse to maintain trust in IoB systems. Given the ethical challenges inherent in the collection, storage, analysis, and use of behavioral data within IoB frameworks, future research should focus on addressing these challenges. Additionally, research should explore the potential psychological impacts of continuous monitoring on patients, the social changes resulting from the adoption of these technologies, and the implications for the patient-healthcare provider relationship. By addressing ethical concerns in the IoB process and implementing policies that ensure equitable access to these technologies, we can advance innovative and smart decision-making while safeguarding human dignity, healthcare efficacy, social welfare, and public health.

REFERENCES

1. Zhao Q, Li G, Cai J, Zhou M, Feng L. A tutorial on internet of behaviors: concept, architecture, technology, applications, and challenges. IEEE Communications Surveys & Tutorials. 2023;25(2):1227-60. Doi: https://doi.org/10.1109/COMST.2023.3246993
2. Shalu, Saini N, Singh M, Kumar JD, editors. The role of the Internet of Behaviours (IoB) in enhancing customer service. 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N); 2023 15-16 Dec. 2023. Doi: https://doi.org/10.1109/ICAC3N60023.2023.10541805
3. Halgekar A, Chouhan A, Khetan I, Bhatia J, Shah N, Srivastava K, editors. Internet of Behavior (IoB): a survey. 5th International Conference on Information Systems and Computer Networks (ISCON); 2021: IEEE. Doi: https://doi.org/10.1109/ISCON52037.2021.9702450
4. Sun J, Gan W, Chao HC, Yu PS, Ding W. Internet of Behaviors: A survey. IEEE Internet Things J. 2023;10(13):11117-34. Doi: https://doi.org/10.1109/JIOT.2023.3247594.
5. Javaid M, Haleem A, Singh RP, Khan S, Suman R. An extensive study on Internet of Behavior (IoB) enabled Healthcare-Systems: Features, facilitators, and challenges. BenchCouncil Transactions on Benchmarks, Standards and Evaluations. 2022;2(4):100085. Doi: https://doi.org/10.1016/j.tbench.2023.100085
6. Amiri Z, Heidari A, Darbandi M, Yazdani Y, Jafari Navimipour N, Esmaeilpour M, et al. The personal health applications of machine learning techniques in the internet of behaviors. Sustainability. 2023;15(16):12406. Doi: https://doi.org/10.3390/su151612406
7. Damaševičius R, Maskeliūnas R, Misra S. Supporting and shaping human decisions through Internet of Behaviors (IoB): Perspectives and implications. In: Adadi A, Motahhir S, editors. Machine Intelligence for Smart Applications: Opportunities and Risks. Cham: Springer Nature Switzerland; 2023. p. 115-44. Doi: https://doi.org/10.1007/978-3-031-37454-8_6
8. Chai PR, Castillo-Mancilla J, Buffkin E, Darling C, Rosen RK, Horvath KJ, et al. Utilizing an ingestible biosensor to assess real-time medication adherence. J Med Toxicol. 2015;11(4):439-44. Doi: https://doi.org/10.1007/s13181-015-0494-8
9. Pasricha S. Ethics for digital medicine: a path for ethical emerging medical IoT design. Computer. 2023; 56(7): 32-40. Doi: https://doi.org/10.1109/MC.2022.3216984
10. Zakerabasali S, Ayyoubzadeh SM. Internet of things and healthcare system: A systematic review of ethical issues. Health Sci Rep. 2022;5(6):e863. Doi: https://doi.org/10.1002/hsr2.863.
11. Mittelstadt B. Ethics of the health-related internet of things: a narrative review. Ethics and Information Technology. 2017;19(3):157-75. Doi: https://doi.org/10.1007/s10676-017-9426-4
12. Ziani L, Khanouche ME, Belaid A, editors. Internet of Behaviors: A literature review of an emerging technology. 2022 First International Conference on Big Data, IoT, Web Intelligence and Applications (BIWA); 2022 11-12. Doi: 10.1109/BIWA57631.2022.10037987
13. Hamid S, Bawany NZ, Sodhro AH, Lakhan A, Ahmed S. A Systematic Review and IoMT Based Big Data Framework for COVID-19 Prevention and Detection. Electronics [Internet]. 2022; 11(17). Doi: https://doi.org/10.3390/electronics11172777
14. Panda N, Perez N, Tsangaris E, Edelen M, Pusic A, Zheng F, Haynes AB. Enhancing Patient-Centered Surgical Care with Mobile Health Technology. Journal of Surgical Research. 2022; 274: 178-84. Doi: https://doi.org/10.1016/j.jss.2022.01.005.

[DOI: 10.22034/ijethics.6.3.64]