Building Digital Trust in Healthcare: Empowering Users to Define their Tracking Boundaries

Mansoor Veliyathnadu Ebrahim

doi: https://doi.org/10.37745/ejcsit.2013/vol13n22232 Published February 12, 2025

Citation: Ebrahim M.V. (2025) Building Digital Trust in Healthcare: Empowering Users to Define Their Tracking Boundaries, *European Journal of Computer Science and Information Technology*, 13 (2), 22-32

Abstract: In the increasingly digital world, trust serves as a cornerstone for consumer interaction, particularly in assuring users that they are engaging with legitimate and reliable applications or platforms. This is particularly crucial within the healthcare sector, where transparency is vital throughout the consumer journey—from plan selection and purchase to the delivery of healthcare services. This article delves into the critical role of digital trust and transparency, addressing prevalent concerns and examining the benefits of building trust and maintaining transparency. Furthermore, it explores technical solutions designed to address these challenges, aiming to enhance patient engagement and improve health outcomes effectively. Data privacy is acknowledged as an important aspect but remains out of the scope of this discussion.

Keywords: digital trust, transparency, digital tracking, privacy concerns

INTRODUCTION

Trust is necessary for every consumer on the digital front because they want to verify whether the application or platform, they are using is the one issued by a company. This is especially important in the healthcare industry, where it is critical to ensure visibility across the entire consumer journey, from purchasing and selecting a plan through to the delivery of services.

In this article, we discuss the importance of digital trust and transparency, the key issues related to it, and the benefits of cultivating trust and transparency. It also covers the technical solutions that can be implemented to address such challenges to build trust for better patient engagement and driving health outcomes. Data privacy is a big consideration but is outside the scope of this article.

Concerns in Digital Tracking

It's widely understood that individuals are being tracked in nearly everything that they do online, which holds true to a certain extent. Digital platforms serve as an effective medium for businesses to gain deeper insights into their customers and their needs. Companies strive to meet these needs as efficiently as possible. In essence, these dynamic, benefits both sides: customers or members enjoy seamless and hassle-free experiences, while businesses can deliver their products or services faster, ensuring customer satisfaction and loyalty.

These advantages can only be realized if digital platforms keep track of every user interaction and navigation. This brings up a significant concern: what about privacy? More precisely, how can users understand the level of tracking these platforms are employing? This is where transparency plays a vital role. By openly sharing their data practices, platforms can foster trust with their users, making sure that consumers feel informed and safe in their online experiences.

Here are some of the key concerns in digital platforms.

- Lack of Transparency and Control:
    - Many platforms fail to offer clear and accessible information regarding the data they collect, its usage, and the parties with whom it is shared. This lack of transparency leaves users in the dark about how much their privacy is at risk. Furthermore, users frequently have few options to opt out of data collection or to delete their information, which complicates their ability to take effective measures to safeguard their privacy. This situation results in a power imbalance, with platforms wielding considerable control over user data without facing any accountability [1].
- Risks of Data Breaches and Overreach:
    - The massive amounts of personal data collected by platforms make them attractive targets for cyberattacks. Data breaches can expose sensitive information, leading to severe consequences such as identity theft, financial loss, and emotional distress. Furthermore, platforms often engage in overreach by collecting more data than necessary for their services, including highly personal details like location, browsing habits, and even biometric data. This excessive collection, combined with poor data management practices, increases the risk of misuse or unauthorized access.
- Third-Party Sharing and Profiling:

  - Many platforms share or sell user data with third parties, such as advertisers or data brokers, without obtaining explicit consent. This practice strips users of control over their personal information and exposes them to further privacy risks. The data collected is often used to create detailed user profiles, which can enable targeted advertising or even discriminatory practices. This is a significant and widespread concern in the healthcare sector, where many individuals fear that being tracked could result in higher costs of care, denial of services, or other negative outcomes.
- Invasive Tracking and Surveillance:
  - Platforms frequently use cross-device tracking to link user activity across smartphones, computers, and other devices, creating a comprehensive picture of their lives without their knowledge or consent. This level of tracking, combined with personalized advertising, can feel intrusive and manipulative, as it exploits user behavior and preferences. The constant sense of being monitored can also lead to a chilling effect, where individuals alter their behavior or refrain from expressing themselves freely due to fear of surveillance.
- Regulatory Gaps and Vulnerable Groups:
  - Privacy laws in many regions are outdated or insufficient to address the complexities of modern digital tracking. This regulatory gap leaves users vulnerable to exploitation and misuse of their data. Certain groups, such as children, are particularly at risk, as they may not fully understand the implications of sharing their data, and platforms often lack adequate safeguards to protect them. In sensitive sectors like healthcare, the stakes are even higher, with concerns about long-term data retention, misuse, and the potential for discrimination based on tracked information. Addressing these issues requires stronger legal frameworks and better enforcement to ensure user privacy is protected.

How Platforms Monitor User Activity and Behavior

You will be amazed to see just how many ways individuals are tracked in the digital world. Below, I've compiled a comprehensive list of the most common tracking methods used by platforms today:

1. Traditional Cookies
   a. Small text files stored on a user's device to track browsing activity, preferences, etc.
   b. Can be session-based (temporary) or persistent (long-term).
2. Location Tracking

   a. IP Address Tracking: Logs users' IP addresses to determine geographic location, device information, and browsing patterns.
   b. GPS and Location Data: Mobile apps access GPS data to track physical location for location-based services and targeted advertising.

3. Behavioral Tracking
   a. Search History and Browsing Data: Tracks queries, visited pages, and time spent on each page to understand user interests and behaviors. [2][3]
   b. Behavioral Analytics: Uses tools like heatmaps, click tracking, and session recordings to analyze how users navigate websites or apps.
   c. App Usage Tracking: Collects data on how users interact with mobile apps, including features used, time spent, and in-app purchases.
   d. Pixel Tracking: Embeds tiny, invisible images in emails or websites to monitor user engagement when content is opened or viewed.
   e. Social Media Tracking: Tracks user interactions (likes, shares, comments, private messages) to build detailed profiles for ad targeting. [4] [6]
4. Cross-Device Tracking
   a. Uses techniques to link a user's activity across multiple devices (e.g., smartphones, tablets, laptops) to create a unified profile. [4]
   b. Device Fingerprinting: Collects information about a user's device (browser type, OS, screen resolution, installed fonts) to create a unique identifier for tracking.
5. Biometric Tracking
   a. Collects biometric information, such as fingerprints or facial recognition data, for authentication or personalization purposes.
   b. Voice and Audio Data: Voice-activated devices and apps (e.g., Alexa, Google Home) may collect and analyze audio data for service improvement or targeted advertising.

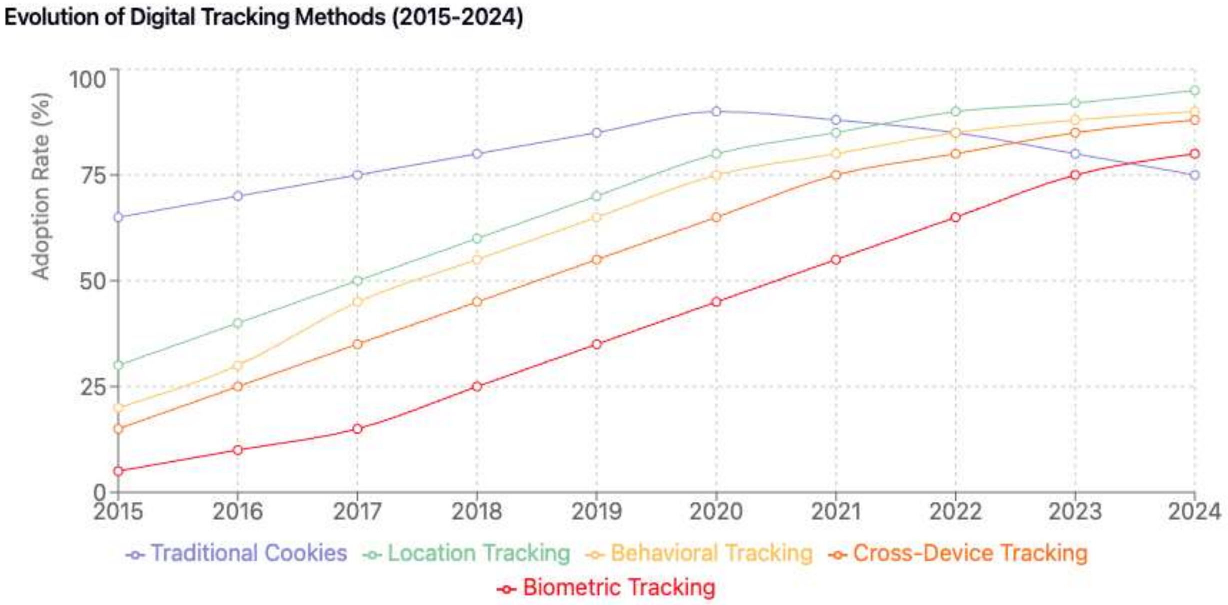


Figure 1: Showing how digital tracking increased over past 10 years

Note that while traditional cookie-based tracking has shown a decline, other forms of tracking continue to grow. This shift is driven by stricter regulatory rules, such as GDPR and CCPA, and changes in browser policies.

Why Digital Trust and Transparency are Vital in Healthcare

Well, digital trust and transparency are essential in every domain, especially critical in healthcare domain to build patient confidence, improve health outcomes, and ensure ethical data practices. When patients trust digital platforms, they are more likely to share accurate information and engage with telehealth services, wearable devices, and health apps, leading to better care management. Transparency about how data is collected, stored, and used protects sensitive health information from breaches and misuse, ensuring compliance with regulations like HIPAA and GDPR. It also reduces patient hesitation in sharing personal information, fostering stronger patient-provider relationships.

The collection and analysis of user data offers numerous benefits, particularly in enhancing user experience and improving health outcomes. By leveraging basic usability data, platforms can optimize interfaces to make them more intuitive and user-friendly. Personalized preventive care reminders ensure that individuals stay on top of their health by receiving timely alerts for check-ups, vaccinations, or screenings. Additionally, personalized coupons or discounts provide users with tailored offers, enhancing customer satisfaction and loyalty. In the healthcare sector, personalized recommendations for medical procedures and providers help individuals make informed decisions, improving the quality of care they receive. Benefits recommendations further assist users in maximizing the value of their health plans or services. Beyond individual benefits, these data, when anonymized, contribute significantly to health research and clinical trials, enabling advancements in medical knowledge and the development of innovative treatments. Additionally, AI can be used for more personalized predictive insights for patients. Overall, the responsible use of data not only enhances personalization and convenience but also drives broader societal benefits in healthcare and research.

Ultimately, trust and transparency are foundational to the success and adoption of digital health solutions, benefiting both individuals and the healthcare system as a whole. Following is some of the related benefits:

METHOD

We carried out a focused study involving a diverse group of participants from different demographics, including both digital and non-digital users, and uncovered the following key insights:

- Members expressed a strong preference for having control over their data, particularly their health records. Members emphasized the importance of having the ability to opt in or out of different types of tracking

- Data security and a lack of transparency regarding how their data is shared.

- Members want clarity on whom their data is shared with and for what purposes.

These findings highlight the need for greater transparency, control, and user-centric approaches in healthcare data tracking. A key insight from our study, conducted with 300 participants, reveals that less than 5% of users today read privacy terms and conditions, with most simply opting to ‘accept’ without fully understanding the policies. However, when provided with a guided and educational experience, 80% of users opted in, demonstrating the importance of clear communication and user-friendly design. Furthermore, 92% of participants expressed a preference for a centralized and guided privacy management system over the current fragmented approaches, highlighting the demand for streamlined solutions. The study also yielded a strong satisfaction score of 4.07, indicating that users value transparency, education, and ease of use when it comes to managing their privacy. These findings underscore the potential for well-designed, user-centric privacy tools to foster greater trust and engagement in the digital landscape

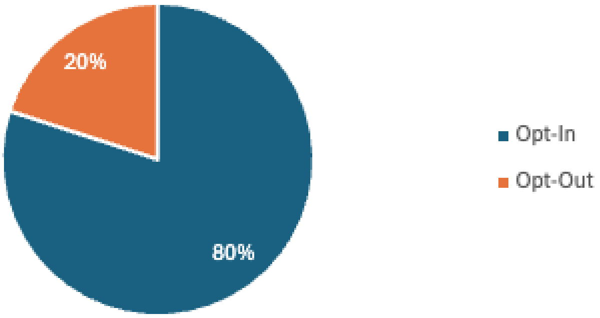
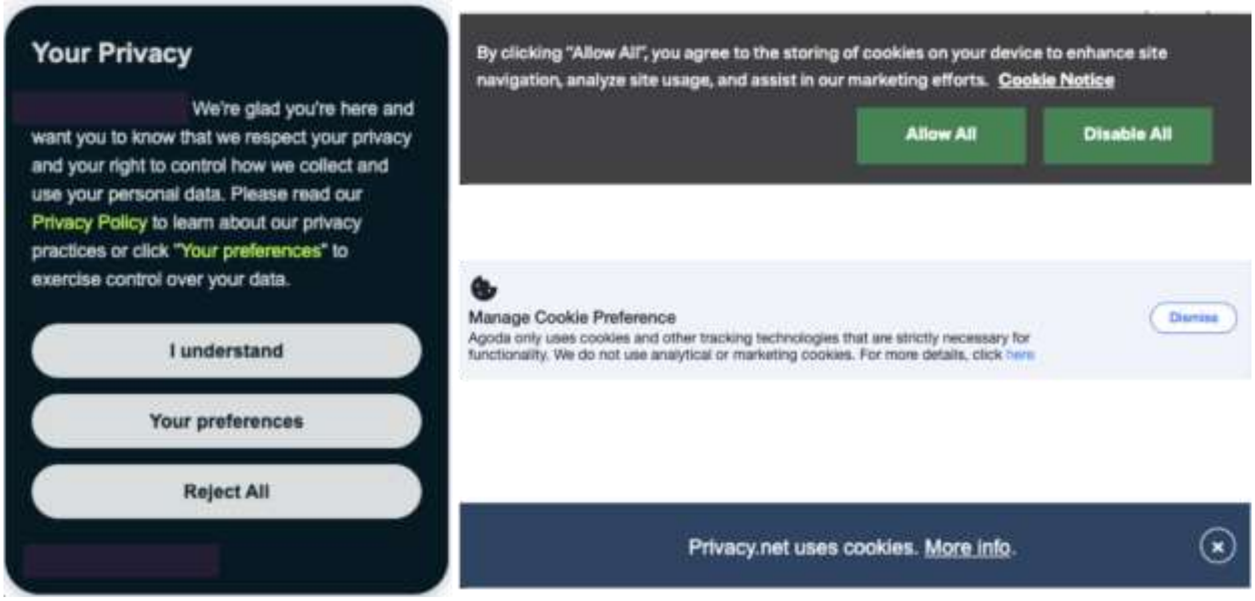


Figure 2: Member Preferences in the Prototype Study

Approach (Architecture and Solution)

There are multiple technical implementations required to bring more trust and transparency to digital platforms. They are discussed as follows.

1. Involve creating a member-friendly interface tailored to the specific platform the member is using, designed to prompt them just before engagement. This prompt clearly outlines each type of data tracking, the level of information being captured, and the purpose of data collection—both for the organization and, more importantly, for improving the member's care management. By providing this transparency upfront, the solution empowers members with knowledge, builds trust, and ensures they understand how their data is used to enhance their care experience.
   a. There are many out of the box solutions available in the market that can be leveraged to get this implemented. Many of these market solutions primarily list individual tracking methods and provide vague explanations, along with an option to opt-in or opt-out. This approach can potentially lead to more opt-outs than opt-ins. Our study suggests that rather than providing a simple list, a guided experience similar to a wizard could help users learn about what is being tracked, how it is used, the benefits, and why opting in is more advantageous than opting out. This increased the trust and adoption rate among our users.



Your Privacy

[redacted] We're glad you're here and want you to know that we respect your privacy and your right to control how we collect and use your personal data. Please read our Privacy Policy to learn about our privacy practices or click "Your preferences" to exercise control over your data.

I understand

Your preferences

Reject All

[redacted]

By clicking "Allow All", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. Cookie Notice

Allow All | Disable All

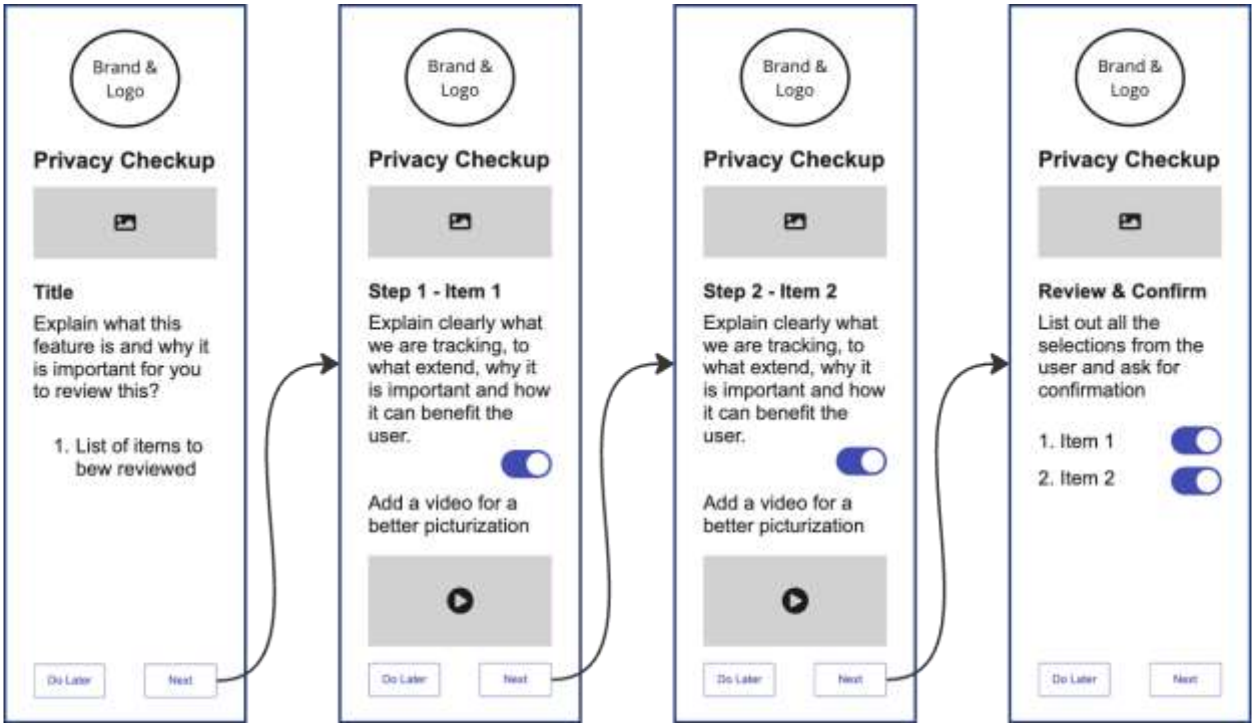
Manage Cookie Preference

Agoda only uses cookies and other tracking technologies that are strictly necessary for functionality. We do not use analytical or marketing cookies. For more details, click here

Dismiss

Privacy.net uses cookies. More info.

Figure 3. Some of the existing or traditional way of asking consensus for tracking users, which is pretty wage and concerning to most of the users



Brand & Logo

Privacy Checkup

Title

Explain what this feature is and why it is important for you to review this?

1. List of items to bew reviewed

Do Later | Next

Brand & Logo

Privacy Checkup

Step 1 - Item 1

Explain clearly what we are tracking, to what extend, why it is important and how it can benefit the user.

Add a video for a better picturization

Do Later | Next

Brand & Logo

Privacy Checkup

Step 2 - Item 2

Explain clearly what we are tracking, to what extend, why it is important and how it can benefit the user.

Add a video for a better picturization

Do Later | Next

Brand & Logo

Privacy Checkup

Review & Confirm

List out all the selections from the user and ask for confirmation

1. Item 1

2. Item 2

Do Later | Next

Figure 4. Proposed wizard experience that can help onboard and educate the members about the different data tracking's and their benefits for being opted in.

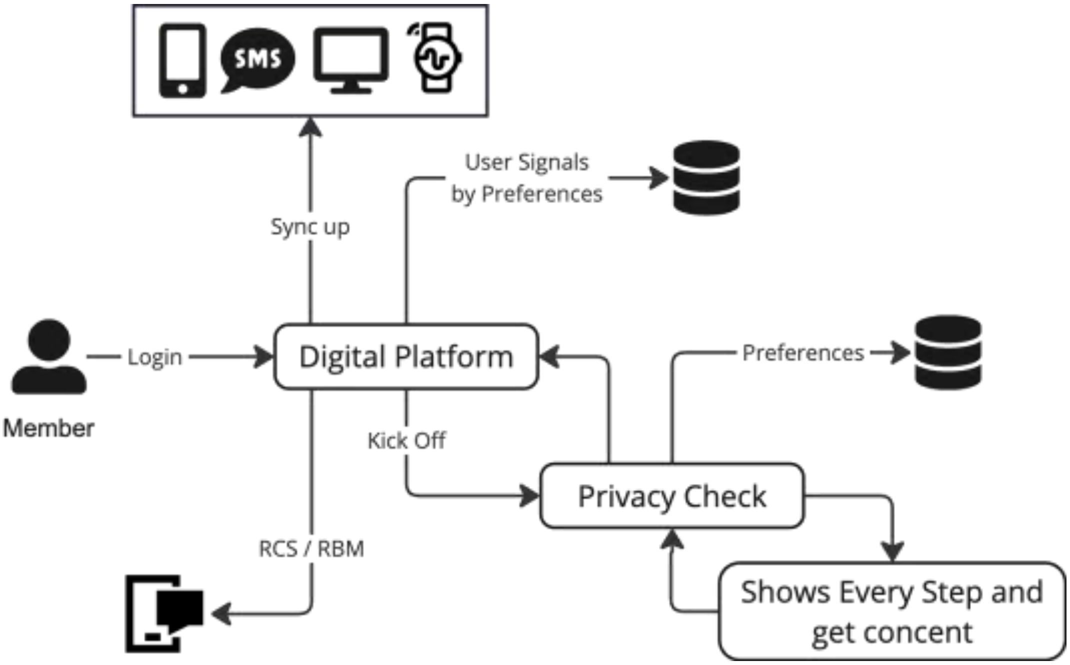


Figure 4. High-level Solution Architecture

2. Branding can significantly enhance digital trust and transparency by establishing a consistent, reliable, and user-focused identity that reassures members their data is handled responsibly. A strong brand communicates credibility and expertise, while clear, accessible messaging about data usage and privacy policies fosters transparency. Consistent branding across platforms creates familiarity, making users feel more comfortable engaging with digital tools and sharing their data. By emphasizing values like privacy, security, and user control, brands can align with user expectations, build emotional trust, and encourage engagement. Ultimately, a trustworthy and transparent brand not only differentiates itself in the market but also fosters long-term loyalty by prioritizing user needs and building confidence in digital interactions.
    a. To build trust, branding should continue to be used in every communication such as Email, Messaging, Call etc., Leverage Google's Rich Business Messaging (RBM) that uses Rich Communication Services (RCS) protocol to create a branded,

enriched communication experience that builds strong trust over these outreach channels.

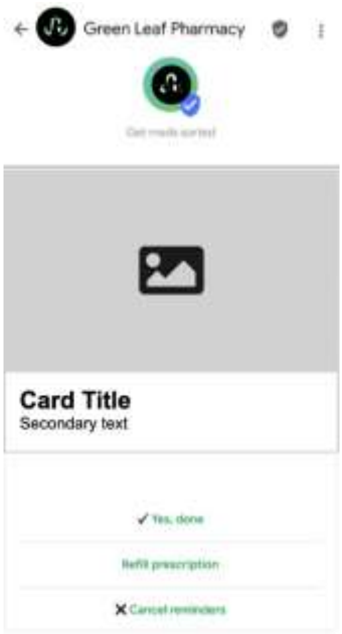


Figure 5: Branding using Rich Communication Services

CONCLUSION

In conclusion, as the digital landscape transforms the healthcare sector, establishing robust digital trust and transparency becomes imperative. By proactively addressing the concerns associated with digital tracking, such as privacy invasion and lack of user control, healthcare platforms can enhance patient engagement and health outcomes. Implementing transparent data practices not only protects sensitive information but also fortifies patient confidence and fosters stronger relationships between patients and providers. The proposed solutions, including user-friendly interfaces and consistent branding, emphasize the importance of clarity and adaptability in data usage. Ultimately, by valuing digital trust and transparency, healthcare platforms can ensure ethical data practices, increase user confidence, and promote the widespread adoption of digital health solutions, contributing positively to the healthcare ecosystem.

REFERENCES

[1] Reshma N.K., Claudia O.R., Igor B., Ernesto D.A., (2021). “Personalization, Privacy, and Me”. doi: 10.48550/arxiv.2109.06990

[2] Nicole M., (2020). "Trusting the bot: Addressing the ethical challenges of consumer digital mental health therapy". doi: 10.1016/bs.dnb.2020.03.003.

[3] Dorian P., Karina V., Diana R., Rafael A. C. (2023). "Responsible AI—Two Frameworks for Ethical Design Practice". doi:10.1109/tts.2020.2974991.

[4] Sarah D., Andreas K., Matthias L., Jasmin N. and Daniel U. (2016), "Technology for Behavior Change – Potential, Challenges, and Ethical Questions". doi:10.1515/icom-2016-0025.

[6] Klaus W. (2021), "Marketing Automation: Marketing Utopia or Marketing Dystopia?" doi: 10.2478/nimmir-2021-0003.