Multidisciplinary Journal of Research in Engineering and Technology
ISSN: 2348-6953
Volume 13 Issue 2 (2026) | Pages: 205-208

A Systematic Literature Review on Digital Footprints: Implications, Risks, and Best Practices

Darshana Yadav[1], Gayatri Ashtikar [2], Namrata Akolkar[3], Pranita Birajdar [4], Prashasti Dhanorkar[5], Prathamesh Karande [6]

[123456]MCA, MES IMCC, Pune, Maharashtra, India

[1]dpy.imcc@mespune.in, [2]ashtikargayatri08@gmail.com, [3]namrataakolkar022@gmail.com, [4]*pranitabirajdar09*@gmail.com, [5]dhanorkarprashasti @gmail.com, [6] prathmeshkarande511@gmail.com

Peer Review Information

***Type**: Article*
***Received:** 18 March 2026*
***Revised:** 01 April 2026*
***Accepted:** 18 May 2026*
***Published:** 01 June 2026*

Abstract

The increase in usage of digital technologies has led to the surge in personal information getting stored on the web. This online presence leaves a mark or data traces, commonly referred to as digital footprints, which are used to access user behaviour, user personality, their thinking patterns and are widely used in many fields. Notwithstanding, the continuous generation and collection of such personal data also raise concerns related to privacy, data misuse, and cyber threats. This study presents a thorough analysis of existing research on digital footprints. A comprehensive set of methodologies used for study show that the volume of data has been increased at a very high rate. This review covers applicable literature from 2015 to 2025 to highlight key patterns in user behaviour. The findings show that even though digital footprints support data-driven decision-making, they also place users at risk of identity theft, cyberbullying, and privacy violations. The review also focuses on the fact of less user awareness and complex policies by platforms. The study highlights requirements for enhanced digital proficiency and awareness amongst individuals, a simplified privacy structure, and stronger data management frameworks. The results provide an integrated overview of current research and emphasize the areas where more work is required in the future for digital footprint protection.

Keywords: Digital Footprint, Data Privacy, Cybersecurity, Online Identity, Cyberbullying, Data Protection

How to Cite This Article

Yadav, D. Ashtikar, G. Akolkar, N. Birajdar, P. Dhanorkar, P. Karande, P. (2026). A Systematic Literature Review on Digital Footprints: Implications, Risks, and Best Practices. *Multidisciplinary Journal of Research in Engineering and Technology*13(2), 205–208.

Introduction

Research Problem

In today's era, users use online platforms for communication, education, entertainment, and business activities. Each of these interactions generates data traces known as digital footprints. These footprints include information produced through browsing activities, social media posting, communication with others and online transactions.

Digital footprints are mainly of two types. Active digital footprints and Passive digital footprints. Active digital footprints are created when users show online activity by sharing information online, such as posting photos or content on social media or submitting personal information on websites on their own. *Passive digital footprints* are produced without permission of the user when websites collect user data through cookies, analytics tools, or background tracking mechanisms.

While digital footprints offer benefits such as improved service personalization and data-driven insights, they also introduce various vulnerabilities. Private information achieved on the web is vulnerable to misuse by cybercriminals for the purposes of identity fraud, cyberbullying, and social engineering. As digital infrastructure continues to expand, the volume of digital footprint data has increased considerably.

Following the COVID-19 pandemic, reliance on digital platforms for remote learning, online collaboration, and digital transactions has grown exponentially. This shift has accelerated the generation of virtual traces, making privacy protection and digital literacy top-tier priority.

Need for Review

Although many studies have explored digital footprints, existing research is scattered across multiple fields including cybersecurity, education, behavioural analytics, and digital identity management. A structured review is necessary to synthesize these findings and deliver overall analysis

This exhaustive review focuses on:

- Summarize existing research on digital footprints
- Examine privacy and cybersecurity risks linked when it comes to online trace data
- Analyze how digital footprints are used by organizations and institutions
- Identify gaps in current literature and propose future research directions

Methodology

This research follows a Systematic Literature Review (SLR) approach to collect and deconstruct existing academic literature related to digital footprints and the risks associated.

Review Process

The review process comprised of four stages prevalently occurred in systematic literature reviews:

1. Identification of relevant studies
2. Screening of titles and abstracts
3. Eligibility assessment using inclusion and exclusion criteria
4. Final selection of studies for detailed analysis

At the outset, a large pool of research articles was identified with authentic academic datasets. After systematic curation, the most relatable studies were used for analysis.

Inclusion Criteria

Research was selected for this review based on the following criteria:

- Oriented towards digital footprints, online identity of users, data sharing, or digital trace data usage
- Addressed data privacy risks, cybersecurity threats, or data protection strategies
- Published in peer-reviewed journals, conference proceedings, or academic reports
- Written in English
- Published between 2015 and 2025

Exclusion Criteria

Studies were excluded if they:

- If they did not focus on digital traces, online identity, data privacy and security
- Were non-academic sources such as blogs/posts or opinion articles
- Lacked sufficient methodological detail

Databases Searched

The literature was collected from the following academic databases:

- Google Scholar
- IEEE Xplore

- SpringerLink
- ScienceDirect
- ResearchGate

Search Query and Relevant Keywords

The search process used combinations of keywords related to digital footprints and data traces and data privacy.
Examples of search queries include:

- "Digital Footprint" AND "Cybersecurity"
- "Digital Identity" AND "Security implications"
- "Data Sharing" AND "Security Constraints"
- "Online Identity" AND "Data Privacy"
- "Digital Footprint Management" AND "User Awareness"
- "Digital Trace Data" AND "Cyber Threats"

Using these queries, approximately over 100 papers were selected. After application of inclusion and exclusion criteria, only 19 studies got selected for deep analysis.

Findings and Thematic Analysis

The thorough analysis of selected literature revealed several prominent themes related to digital footprints.

Generation of Digital Footprints

Digital footprints are created through everyday digital activities such as browsing websites, interacting on social media, participating in online discussions, form submissions, E-Commerce usage, location services, IoT and smart devices and conducting digital transactions. This includes what we look at on the internet, what we do on media and what we buy online. Sometimes we make these footprints on purpose like when we sign up for a website or post a comment. At times they happen without us even knowing it. Both active and passive data traces contribute to the accumulation of personal information online. Researchers emphasize that even small actions, such as clicking links or searching for information, contribute to a user's digital identity. Now, AI systems are also using these digital footprints to predict the behaviour of the consumers for real world scenarios.

Privacy and Security Risks

One of the important things in the literature is to consider the potential misuse of digital footprint data. Personal information stored online can be exploited by cybercriminals for activities such as identity misuse, and targeted harassment. In addition, digital footprints are used to generate detailed user profiles, which may raise ethical concerns regarding surveillance and privacy violations.

Use of Digital Footprints by Organizations

Data brokers frequently analyze digital footprints to understand user behaviour and improve services. Data retrieved from online activity can be used for targeted advertising, market research, and customer experience enhancement. Nowadays, recruiters check the social media presence of the candidates while hiring. Advanced technologies such as machine learning algorithms and data analysis are widely used to analyze large volumes of digital trace data and identify pattern-of-life information.

Lack of User Awareness

A large portion of users are unaware of how their data is being used. The privacy policies and conditions provided by websites are often long and complex, leading users to accept them without fully understanding the implications. This lack of digital literacy increases the chances of unintentional data exposure.

Vulnerable User Groups

Children, teenagers, and adults, are identified as being at a higher risk regarding their digital presence. Younger users may share personal information on social media without understanding potential consequences such as cyber bullying. Older users may lack familiarity with digital privacy settings and can be an easy target for romance scams, confidence fraud and tech support ruses. Unorganized workers often lack standard corporate training making them a high-risk group for business breaches.

Discussion

Literature Gaps

Despite extensive research on digital footprints, there are still a number of significant gaps in the body of knowledge.
First, little study has been done on how to make privacy regulations easier to understand for users. A lot of policies contain legal and technical jargon that is hard for regular users to comprehend. Additionally, privacy policy implementation is not user-friendly.
Second, not enough attention has been paid to the lack of digital literacy among younger and older users. Due to their lack of knowledge about data and privacy dangers, these individuals are usually more prone to online threats.
Third, there is insufficient research on user-centered consent mechanisms that allow individuals to manage their data collection and usage.
Fourth, the research also remained very limited on Gender specific data flow that emphasizes the gender role in online identity and privacy risks associated.
Finally, existing research often highlights the focus on technical solutions but pays less attention and less research to the educational and policy aspects of digital footprint management.

Trends and Associated Future Research Paths.

Recent studies indicate substantially emerging trends in the management of digital footprints.

One prominent trend is the use of AI and ML tools to study digital behaviour and detect cybersecurity threats in early stages. These technological advancements enable large- scale analysis of online activity patterns and their implications.

Another vital direction is the development and regulation of privacy-enhancing technologies, such as tracking prevention techniques and secure data storage systems.

Also there should be proper regulations and governance on the digital data- usage by the companies or organizations and robust measures should be implemented for the clarity of these rules to the users. 19

Further research in this context should also emphasize on improving digital literacy programs, particularly within schools, colleges, universities and the general public should also be considered. Educating users about data collection, digital privacy and responsible online behaviour can significantly reduce the risks associated with digital footprints.

Collaboration amongst technologists, educators, and policymakers is going to play a prominent role for developing impactful plans to protect users while still enabling technological innovation.

Conclusion

Digital footprints are an unavoidable byproduct of modern digital interactions. Although they give us important information for organizations and researchers, they also present significant privacy pitfalls and security gaps.

This review analyzed existing studies to understand how digital footprints are generated, how they are used, and what risks they pose to individuals.

The findings highlight that lack of social engineering training, complex privacy policies, and large-scale data collections contribute to the misuse of digital footprint data. Focusing on these problems requires a combination of technological solutions, policy reforms, and educational initiatives.

Improving digital literacy, simplifying privacy policies, and strengthening protection regulations can help data-safety rules and regulations help individuals to have better control over their digital identities. By promoting responsible data practices and increasing awareness of digital footprints, it is possible to develop a safer and more secure digital ecosystem.

References

1. Timmis, S., Broadfoot, P., Sutherland, R., & Oldfield, A. (2016). *Rethinking assessment in a digital age: Opportunities, challenges and risks.* British Educational Research Journal.
2. Sjöberg, M., Chen, H., Floreen, P., et al. (2017). *Digital Me: Controlling and Making Sense of My Digital Footprint.*
3. Leonardi, P. M. (2021). *COVID-19 and the New Technologies of Organizing: Digital Exhaust, Digital Footprints, and Artificial Intelligence.*
4. McDermot, M. (2018). *Digital Footprints: Creation, Implication, and Higher Education.*
5. Oatley, G., Crick, T., & Mostafa, M. (2015). *Digital Footprints: Envisaging and Analysing Online Behaviour.*
6. Osborne, N., & Connelly, L. (2015). *Managing Your Digital Footprint.*
7. A. M. Alshehri (2016). Digital Footprint: End Users' Data Privacy Concerns 30.
8. Ketipov, R., Schnalle, R., Doukovska, L., & Dehez, D. (2024). *Managing Cybersecurity: Digital Footprint Threats.*
9. Attitudes Towards Sharing Digital Footprint Data, McDonald, R., Skatova, A., & Maple, C. (2023).
10. Dutt, B. (2023). *Wellbeing Amid Digital Risks.*
11. Kapliar, K. *Cybersecurity in Neobanks: New Risks and Solutions.*
12. Pilgun, M. (2025). *Digital Footprints from Social Networks.*
13. Berg, V., et al. (2024). *Young Children and Digital Identity on Social Networking Sites.*
14. Tremper, K. A. *Our Digital Footprint: Protecting the Next Generation.*
15. Cheng, F. C., & Wang, Y. S. (2018). *Do-Not-Track Mechanism for Digital Footprint Privacy Protection.*
16. Wook, T. S. M., et al. (2019). *Awareness of Digital Footprint Management Among Youth.*
17. Aguiar, J. (2024). *Digital Footprint Management and Youth Social Media Usage.*
18. Mathew, A. (2023). *Cybersecurity Data Science in Protecting Digital Footprints.*