eISSN 2583-6986

IDEALISTIC JOURNAL OF ADVANCED RESEARCH IN PROGRESSIVE SPECTRUMS (IJARPS)
A MONTHLY, OPEN ACCESS, PEER REVIEWED (REFEREED) INTERNATIONAL JOURNAL
Volume 04, Issue 08, August 2025

A Study on Digital Footprints and Concerns About Privacy and Security on Social Media

Dr. Prakriti Dixit Porwal[1], Nitin Kasera[2], Limra Khan[2] and Priyanshi Kumawat[2]
[1]Associate Professor, Department of Management Studies, Geetanjali Institute of Technical Studies
[2]Students, Department of Management Studies, Geetanjali Institute of Technical Studies

Received: 20 August 2025 Accepted & Reviewed: 25 August 2025, Published: 31 August 2025

Abstract

Now-a-days life takes place in the digital world more than ever before. The pervasiveness of online platforms for social networking, banking, shopping, and other purposes in the current digital era illustrates how big data and digitalization are becoming progressively more ingrained into our daily lives, changing the way we engage with the outside world and carry out our daily tasks. The digital footprint left by online personal information disclosure raises serious questions regarding data security and the safeguarding of users' private data. This study looks at how shared personal data turns into an enduring digital record that may be investigated and possibly manipulated by third parties including hackers, businesses, etc.

It attempts to offer insights into methods for reducing these risks through improved privacy settings, regulated information exchange, and knowledgeable digital habits to protect personal data by investigating users' perceptions of the main data hazards.

The objective of research is to highlight the vulnerabilities and risks inherited in digital footprint. The findings of this study are intended to educate online users and developers on the vital significance of protecting private data and strengthening privacy safeguards in order to reduce security threats in the digital age. This study aims to create a safer digital environment that protects user privacy and encourages responsible data management by identifying issues and offering workable solutions.

Keywords: Online Era, Digital Footprint, Security Risk, Privacy Protection

Introduction

The emergence of the global web in the late 20th century marked the beginning of the online era, which transformed information sharing, communication, and business. By ensuring digital interactions, encouraging innovation, and building a more connected world, it sought to unite people worldwide, provide quick access to data, and revolutionize businesses. Similar to how a person leaves footprints when they walk, a person's online activities create a “digital footprint” that is a record of their interactions, browsing habits, and data exchanged on the internet. Privacy, security, and customized services are impacted by this footprint, which provides information about an individual's habits, preferences, and interests.

Social media's widespread use has created a complicated web of digital footprints that record a wide range of online preferences, behaviours, and activities in distinctive and dynamic ways. Businesses looking to learn more about the psychological profiles and behaviors of their customers can benefit greatly from these digital footprints, which are frequently left unnoticed. A recent study explores if it is possible to predict personality traits from traces people leave on social media alone. Individuals' use of social media platforms like Facebook, Instagram, and Twitter has become nearly instinctive, adding to an expanding data ecology, even if they may not be conscious of the digital footprints they leave behind. Google, Amazon, Facebook, and other social media businesses have mastered the art of tracking user behaviour through advanced scanning techniques, gathering personal information from users' online activities. Businesses use the insightful information acquired from such data's analysis deploying complex algorithms to improve their marketing tactics, customize content, and increase customer engagement. Business value creation has been transformed by the ongoing analysis of user-generated data, which enables organizations to predict customer preferences and demands with amazing accuracy.

Collecting digital footprints has become essential to obtaining a competitive edge as businesses fight to stay ahead. In addition to helping managers better understand consumer behaviour, these massive data sets can also spur innovation, improve customer satisfaction, and advance company expansion. Digital footprints are therefore a crucial instrument in determining how corporate strategy and value generation will develop in the future.

But even with the advantages of digital footprints, an online market has a negative aspect. Because consumers frequently aren't aware of how much their information is being used, the massive collection and analysis of personal data raises serious privacy concerns. As malevolent actors target sensitive data, fraudulent activities like identity theft and data breaches have increased dramatically. Trust in digital platforms is further weakened when companies or unapproved third parties misuse personal data, which can result in exploitation and manipulation. As a result, it is more important than ever to have strong privacy protections and moral data management procedures.

Objectives Of Research-

A digital footprint can determine a person's digital reputation, which is now considered as important as their "offline" reputation. Through this research we are trying to address these objectives.

- Accessing the privacy risk, identifying the privacy risk associated with the digital footprint on social media platforms.
- User awareness and behaviour, investigating the level of awareness users have regarding their digital footprint and how this impacts their online behaviour.
- Addressing privacy management strategies analyse how users manage their privacy settings and their effectiveness of these strategies in protecting their personal information.
- Understanding digital footprint and examine what constitutes a digital footprint and how user actions on social media contribute to it.
- Recommendations for users to protect their privacy and suggestions for policymakers to enhance data protection laws.

Digital Footprint-

A digital footprint is the collection of information resulting from online activities including email correspondence, social media engagements, and website visits. To protect privacy and maintain a good online reputation, it is essential to manage one's digital footprint. It can result in identity theft, reputational harm, and privacy issues if left unchecked.

Let's look into various ways to manage:

- Track Internet Activity: Search your name frequently to find information that is accessible to the public and take action to remove any inaccurate or undesirable stuff.
- Use Strong Passwords: To improve security, create distinct, complicated passwords for every account that combine letters, numbers, and special characters.

- Modify Privacy Settings: To limit the visibility of personal data, check and modify privacy settings on social media sites.

Solutions for Enhanced Control:

- Regular Audits: Periodically check your digital presence by detecting obsolete, irrelevant, or unsuitable content and taking corrective action, such as removing or updating information.
- Data Management solutions: To prevent data misuse, employ software solutions that include functions like digital footprint tracking, password management, and privacy alerts.

Actively managing digital footprints promotes a more secure and polished online persona in addition to safeguarding private data.

Security Risk-

Security risks encompass potential threats to the confidentiality, integrity, and availability of information. These risks can stem from cyber-attacks, data breaches, and malware infections. Mitigating security risks involves several proactive measures. Installing up-to-date anti-virus software, enabling two-factor authentication (2FA), and being vigilant about phishing attempts are essential practices. Additionally, regular software updates and the use of secure networks can significantly reduce the vulnerability to security threats. Implementing robust network security protocols is also vital in protecting sensitive information.

Here are effective strategies to reduce online security risks.

- Install Anti-Virus Software: Protect your devices with up-to-date anti-virus software.
- Enable Two-Factor Authentication (2FA): Add an extra layer of security to your accounts by requiring a second form of verification.
- Be Wary of Phishing: Avoid clicking on suspicious links or providing personal information through unverified sources.

Effective Solutions to Mitigate Security Risks:

- Regular Software Updates: Keep all your software and operating systems up to date to protect against vulnerabilities.
- Network Security: Use secure and encrypted networks, especially when accessing sensitive information.

Privacy Protection-

Privacy protection involves safeguarding personal information from unauthorized access and misuse. Limiting data sharing and using secure browsers and Virtual Private Networks (VPNs) are fundamental practices for enhancing privacy. Encryption of sensitive data, both in transit and at rest, is crucial for protecting personal information. Compliance with privacy legislation ensures that data handling practices meet established standards, further safeguarding individuals' privacy.

Let's examine various tactics to strengthen and enhance privacy:

- Limit Data Sharing: Only share personal information with trusted websites and services.
- Use Secure Browsers and VPNs: Enhance your online privacy with secure web browsers and Virtual Private Networks (VPNs).

Solutions:

- Encryption: Ensure that sensitive data is encrypted both in transit and at rest.
- Privacy Legislation Compliance: Familiarize yourself with privacy laws and ensure compliance to protect personal data.

Review Of Literature-

In the fields of academia and industry, the idea of digital footprints has attracted a lot of interest, particularly in relation to cybersecurity, online privacy, and personal identity management.

The importance of controlling one's digital identity is emphasized by Christian (2024), who also highlights methods for safeguarding digital footprints by using network security protocols and frequent software updates. In addition to offering useful strategies to reduce security concerns in the digital age, this guide offers a thorough grasp of the hazards that come with digital footprints.

Golder and Macy (2014) highlight the advantages and disadvantages of digital footprints for data collecting and analysis in the context of social research. While recognizing the ethical ramifications and privacy issues associated with using such data for academic purposes, their work highlights the potential of digital footprints to support extensive online social research.

By examining the new idea of digital inequality, Micheli, Lutz, and Büchi (2018) broaden the discussion on digital footprints. They contend that people who lack access to digital tools or knowledge are clearly at a disadvantage when it comes to maintaining their online appearance, and that digital footprints can worsen already-existing socioeconomic disparities. This emphasizes how crucial it is to take ethical considerations into account when researching privacy and digital footprints.

Osborne and Connelly (2015) look into the effects of controlling digital footprints in learning environments. With relation to students' online personas and the learning resources they employ, their research focuses on the potential impact of digital identity management on instruction and learning.

Kligienė (2012) presents a distinct stance, emphasizing the relationship between professional ethics and digital traces. Particularly with regard to privacy and the appropriate use of digital information, this work advances our understanding of how professionals might negotiate the ethical dilemmas presented by online data trails.

Weaver and Gahegan (2007) offer a spatial viewpoint on digital footprints, going over the various ways that digital traces can be created, displayed, and examined. By showing how spatial data can interact with online activities to provide deeper insights into user behaviours, this research establishes the foundation for the geographical analysis of digital footprints.

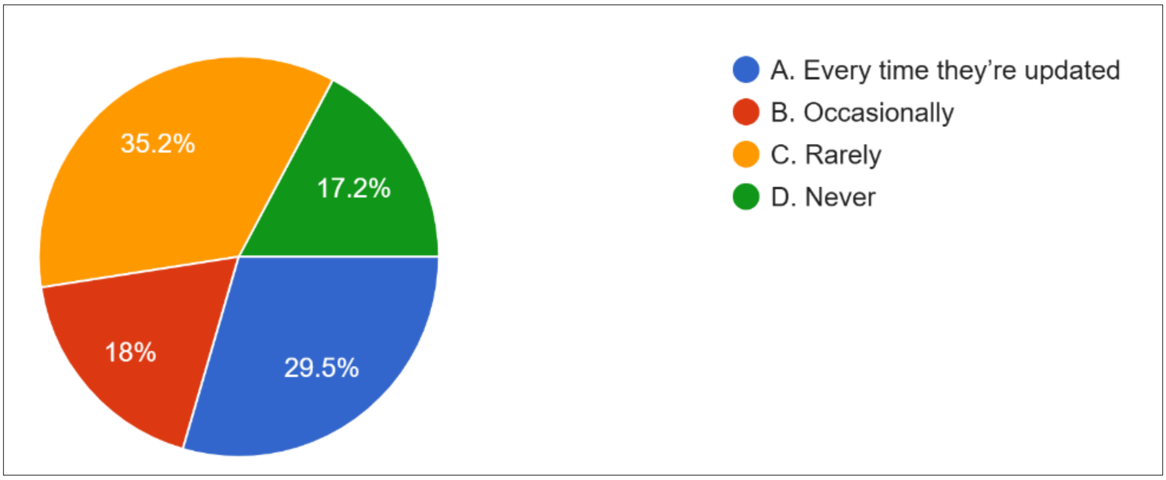
In their meta-analysis of the use of digital footprints for personality analysis, Azucar, Marengo, and Settanni (2018) concentrate on the predictive power of digital footprints on social media for personality traits like those listed in the Big Five personality model. This study demonstrates how digital footprints can be a valuable source of behavioural and psychological information.

Collectively, these studies demonstrate how digital footprints are complex, involving privacy, security, societal ramifications, and ethical issues. As digital technologies continue to advance and permeate every facet of life, the literature as a whole emphasizes the significance of appropriately maintaining one's digital stamp.

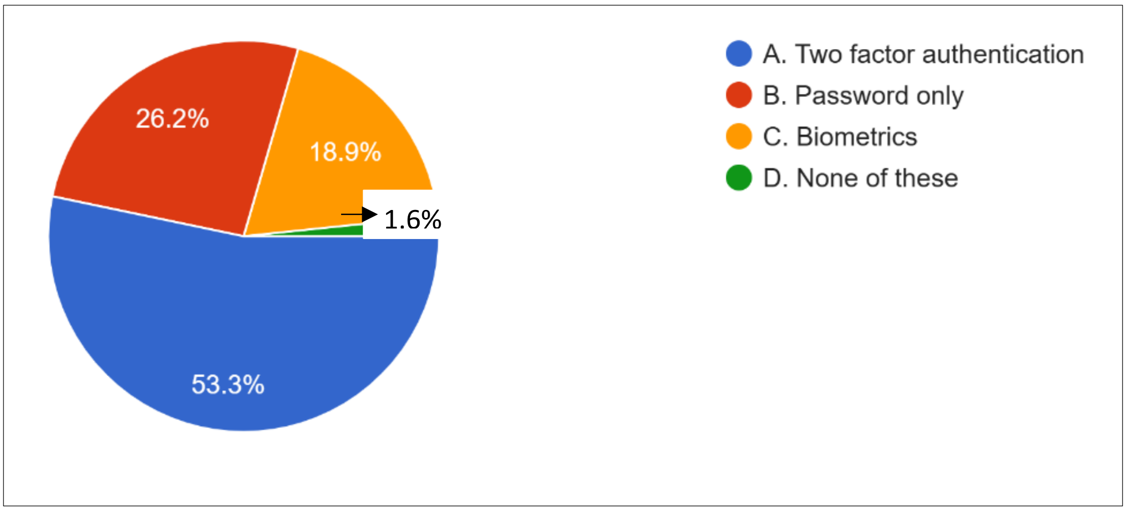
Research Methodology -

The study collects data from both primary and secondary sources. A structured Google Form questionnaire was used to collect primary data from 122 participants. The questionnaire was created to extract pertinent replies through a sampling technique. A thorough grasp of the subject was provided by the secondary material that was gathered from a variety of reliable sources, such as websites and research papers.

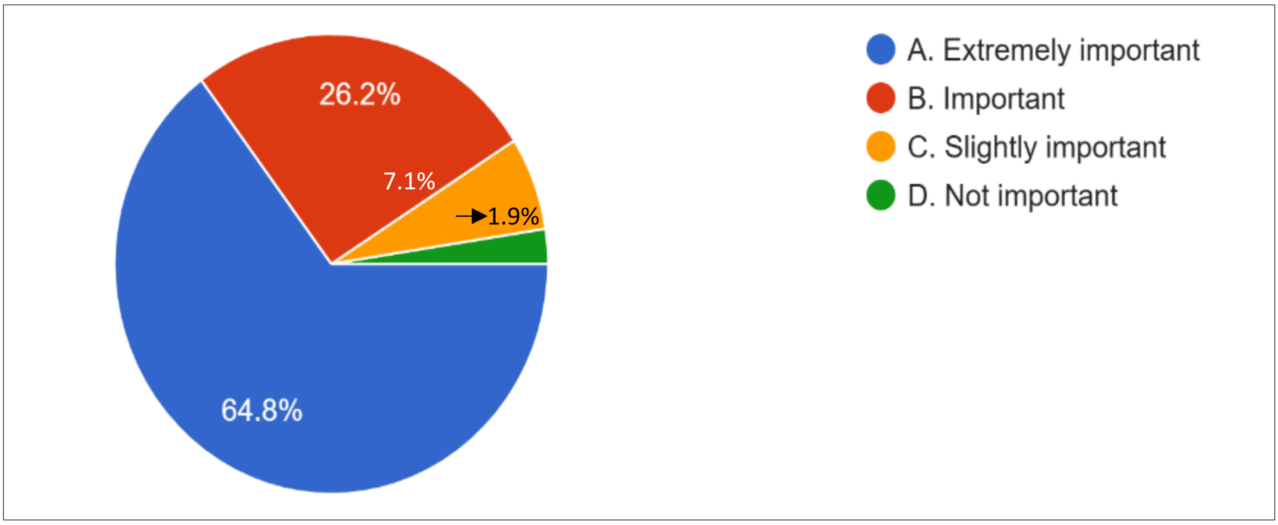
Analysis And Interpretation -



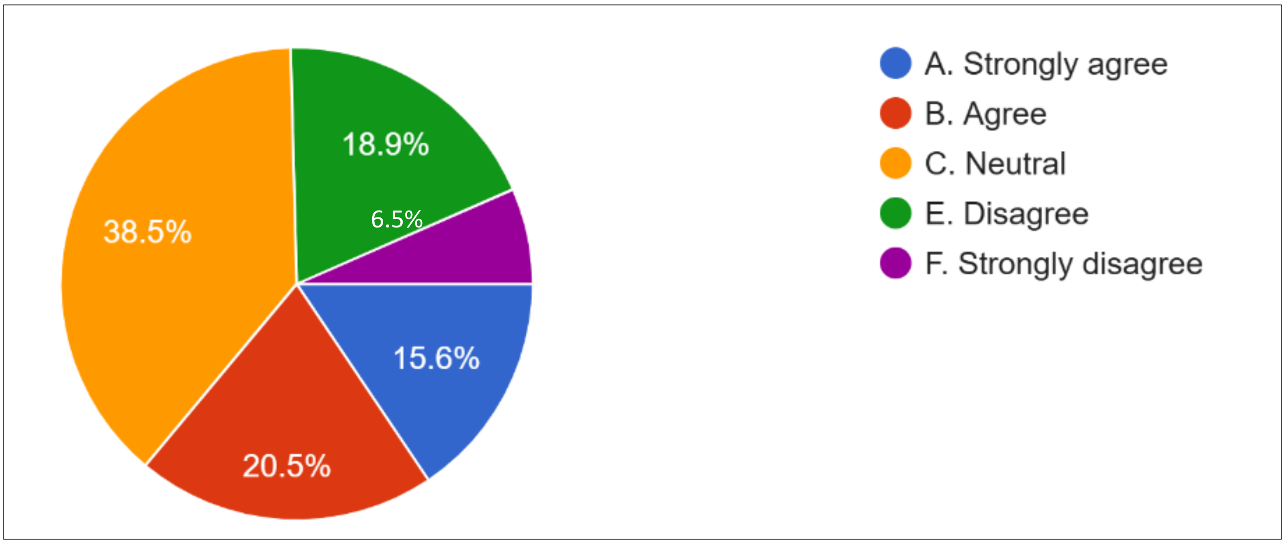
The conclusion of the questionnaire on reading habits for social media privacy policies are displayed in the illustration above. According to the survey responses, a sizable percentage of participants (35.2%) check out social media privacy policies whenever they are altered. But a sizable portion (29.5%) never reads them. The remaining participants read them infrequently (17.2%) or occasionally (18%). According to these statistics, many users appear to be unaware of or unconcerned with social network privacy policies. While certain individuals place a high value on being aware of privacy practices, a greater percentage either never reads them or only occasionally does. Users may unintentionally accept agreements that risk their data security and personal information as a result of this indifference, which might result in privacy problems.



Security for social media accounts provides protection for personal profiles on the internet from unwanted access. Strong passwords, biometrics such as fingerprint or face ID, and two-factor authentication like OTPs are some of the techniques. Encryption, device tracking, and security questions are extra precautions. According to the data collected, which is represented in the pie chart above, 53.3% of participants use passwords, 26.2% use two-factor authentication, 18.9% use biometrics, and 1.6% do not use any security measures. The use of passwords, which are less secure than multi-factor authentication, is alarming. Users are exposed to risks like hacking and identity theft because of their lack of awareness of digital security. Protecting personal information while assuring privacy online require raising awareness and advocating the implementation of advanced safety solutions



The above illustration shows how important individuals consider data privacy while using social media. According to the survey, a sizable majority of participants (64.8%) believe that data privacy is crucial when using social media. On other hand a small percentage (9.0%) think it slightly or not important, and a smaller percentage (26.2%) think it is vital. It indicates that social media users are becoming more conscious of and concerned about data privacy. This finding reveals a change in user perceptions and expectations, has inspired social media platforms to place greater focus on data security and transparency. To ensure ethical handling of data operations, it also highlights the significance of strong privacy laws and user education.



The respondents' opinions regarding social media companies' adherence to safeguard user privacy are represented in the figure above. Based on response collected, respondents do not trust social media firms to preserve their privacy. A sizable majority (59.4%) express disagreement or stronly disagreement with the statement, expressing worries about privacy and data security procedures. Compared to just 20.1% who agree or strongly agree, a smaller percentage (20.5%) are neutral. This information suggests that individuals are generally suspicious of social media businesses' confidentiality agreements. According to the majority of respondents, these businesses are not very good at protecting personal data. This lack of trust highlights the necessity for social media companies to be more accountable, transparent, and to implement strong privacy policies in order to win back user trust and create a safer online environment.

Hypotheses:

H_{01}: There is no significant impact of Digital Footprints and Concerns about Privacy and Security on Social Media according to given below parameters.

H_{A1}: There is a significant impact of Digital Footprints and Concerns about Privacy and Security on Social Media according to given below parameters.

1. I feel informed about how social media uses my data.

2. I monitor my digital footprint actively.

3. I frequently review my privacy settings to protect my information.

4. I believe I have control over the data I share online.

5. I am confident in social media platforms' commitment to data privacy.

6. I think it's essential to educate people on managing their digital footprint.

7. I would advocate for increased privacy protections in social media policies.

8. I worry about my data security on social media.

9. I am comfortable with companies using my data for personalized advertising.

10. I feel that privacy is a fundamental right in the digital world.

Table 1:

Descriptives									
		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
1. I feel informed about how social media uses my data.	Strongly Disagree	36	3.44	1.403	.234	2.97	3.92	1	5
	Disagree	30	3.87	.900	.164	3.53	4.20	2	5
	Neutral	23	3.83	1.072	.224	3.36	4.29	2	5
	Agree	25	3.60	1.080	.216	3.15	4.05	2	5
	Strongly Agree	9	3.67	1.225	.408	2.73	4.61	1	5
	Total	123	3.67	1.150	.104	3.46	3.87	1	5
2. I monitor my digital footprint actively.	Strongly Disagree	36	3.50	1.207	.201	3.09	3.91	1	5
	Disagree	30	3.67	.922	.168	3.32	4.01	2	5
	Neutral	23	3.43	1.037	.216	2.99	3.88	1	5
	Agree	25	3.60	.866	.173	3.24	3.96	1	5

	Strongly Agree	9	3.78	.667	.222	3.27	4.29	3	5
	Total	123	3.57	1.001	.090	3.39	3.75	1	5
3. I frequently review my privacy settings to protect my information.	Strongly Disagree	36	3.78	1.124	.187	3.40	4.16	1	5
	Disagree	30	3.73	1.048	.191	3.34	4.12	1	5
	Neutral	23	3.65	1.152	.240	3.15	4.15	1	5
	Agree	25	3.64	.952	.190	3.25	4.03	2	5
	Strongly Agree	9	3.67	.707	.236	3.12	4.21	2	4
	Total	123	3.71	1.038	.094	3.52	3.89	1	5
4. I believe I have control over the data I share online.	Strongly Disagree	36	3.42	1.204	.201	3.01	3.82	1	5
	Disagree	30	3.47	1.106	.202	3.05	3.88	2	5
	Neutral	23	3.17	1.114	.232	2.69	3.66	1	5
	Agree	25	3.28	1.100	.220	2.83	3.73	1	5
	Strongly Agree	9	3.89	.928	.309	3.18	4.60	2	5
	Total	123	3.39	1.121	.101	3.19	3.59	1	5
5. I am confident in social media platforms' commitment to data privacy.	Strongly Disagree	36	2.89	1.090	.182	2.52	3.26	1	5
	Disagree	30	3.17	1.117	.204	2.75	3.58	1	5
	Neutral	23	3.04	1.224	.255	2.51	3.57	1	5
	Agree	25	3.00	.913	.183	2.62	3.38	1	5
	Strongly Agree	9	3.22	.833	.278	2.58	3.86	2	4
	Total	123	3.03	1.063	.096	2.84	3.22	1	5
6. I think it's essential to educate people on managing their digital footprint.	Strongly Disagree	36	4.25	1.251	.208	3.83	4.67	1	5
	Disagree	30	4.03	.999	.182	3.66	4.41	2	5
	Neutral	23	3.83	1.114	.232	3.34	4.31	2	5
	Agree	25	4.16	1.106	.221	3.70	4.62	2	5
	Strongly Agree	9	4.11	.782	.261	3.51	4.71	3	5
	Total	123	4.09	1.101	.099	3.89	4.29	1	5

7. I would advocate for increased privacy protections in social media policies.	Strongly Disagree	36	4.00	1.121	.187	3.62	4.38	1	5
	Disagree	30	3.67	.994	.182	3.30	4.04	2	5
	Neutral	23	3.87	1.290	.269	3.31	4.43	2	5
	Agree	25	4.20	.866	.173	3.84	4.56	2	5
	Strongly Agree	9	3.89	.782	.261	3.29	4.49	3	5
	Total	123	3.93	1.057	.095	3.74	4.12	1	5
8. I worry about my data security on social media.	Strongly Disagree	36	3.78	1.245	.207	3.36	4.20	1	5
	Disagree	30	3.90	.923	.168	3.56	4.24	2	5
	Neutral	23	3.74	1.054	.220	3.28	4.19	2	5
	Agree	25	4.12	.881	.176	3.76	4.48	2	5
	Strongly Agree	9	4.22	.667	.222	3.71	4.73	3	5
	Total	123	3.90	1.028	.093	3.72	4.09	1	5
9. I am comfortable with companies using my data for personalized advertising.	Strongly Disagree	36	2.64	1.046	.174	2.28	2.99	1	5
	Disagree	30	3.00	1.259	.230	2.53	3.47	1	5
	Neutral	23	2.96	1.461	.305	2.32	3.59	1	5
	Agree	25	2.76	1.128	.226	2.29	3.23	1	5
	Strongly Agree	9	2.67	1.323	.441	1.65	3.68	1	5
	Total	123	2.81	1.210	.109	2.60	3.03	1	5
10. I feel that privacy is a fundamental right in the digital world.	Strongly Disagree	36	4.19	1.238	.206	3.78	4.61	1	5
	Disagree	30	4.07	1.143	.209	3.64	4.49	1	5
	Neutral	23	3.96	1.022	.213	3.51	4.40	2	5
	Agree	25	4.00	1.118	.224	3.54	4.46	2	5
	Strongly Agree	9	4.22	.972	.324	3.48	4.97	3	5
	Total	123	4.08	1.121	.101	3.88	4.28	1	5

Table 2:

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
1. I feel informed about how social media uses my data.	Between Groups	3.673	4	.918	.687	.002
	Within Groups	157.660	118	1.336		
	Total	161.333	122			
2. I monitor my digital footprint actively.	Between Groups	1.288	4	.322	.314	.868
	Within Groups	120.874	118	1.024		
	Total	122.163	122			
3. I frequently review my privacy settings to protect my information.	Between Groups	.397	4	.099	.089	.986
	Within Groups	131.066	118	1.111		
	Total	131.463	122			
4. I believe I have control over the data I share online.	Between Groups	3.818	4	.955	.754	.557
	Within Groups	149.450	118	1.267		
	Total	153.268	122			
5. I am confident in social media platforms' commitment to data privacy.	Between Groups	1.636	4	.409	.354	.841
	Within Groups	136.234	118	1.155		
	Total	137.870	122			
6. I think it's essential to educate people on managing their digital footprint.	Between Groups	2.746	4	.687	.558	.694
	Within Groups	145.270	118	1.231		
	Total	148.016	122			
7. I would advocate for increased privacy protections in social media policies.	Between Groups	4.177	4	1.044	.932	.048
	Within Groups	132.164	118	1.120		
	Total	136.341	122			

8. I worry about my data security on social media.	Between Groups	3.277	4	.819	.770	.047
	Within Groups	125.553	118	1.064		
	Total	128.829	122			
9. I am comfortable with companies using my data for personalized advertising.	Between Groups	2.877	4	.719	.483	.748
	Within Groups	175.822	118	1.490		
	Total	178.699	122			
10. I feel that privacy is a fundamental right in the digital world.	Between Groups	1.169	4	.292	.227	.923
	Within Groups	152.018	118	1.288		
	Total	153.187	122			

Informed about Social Media Data Usage: The statement "I feel informed about how social media uses my data" shows a neutral to slightly positive response across the groups, with a mean of 3.67. The group of individuals who strongly disagreed with the statement had the lowest mean score (3.44), while those who disagreed were slightly more informed, with a mean of 3.87. The ANOVA test results (p = 0.002) suggest a significant difference between groups, indicating that people who felt more informed about their data usage are more likely to have a higher opinion on the matter.

Monitoring Digital Footprint: When it comes to monitoring digital footprints, the overall mean score of 3.57 indicates a neutral stance. However, responses are more varied across groups. Those who strongly disagreed or disagreed (means ranging from 3.43 to 3.78) have somewhat different levels of active monitoring behavior. The ANOVA test (p = 0.868) indicates no significant difference between the groups, suggesting that the behavior of monitoring digital footprints is fairly uniform across different levels of agreement with the statement.

Privacy Settings and Control: With an average score of 3.71, participants demonstrate a moderate level of privacy settings awareness and action over their visits on various websites. The fact that there is a significant difference between the groups (p = 0.048) indicates that those who strongly agree or disagree behave differently. This emphasizes how specific education is required to enhance privacy practices for all populations.

Data Control and Trust: Respondents' opinions regarding their control over information posted online are conflicted (mean = 3.39). People who strongly agree or disagree have different views of control, as illustrated by the significant difference between groups (p = 0.557). This emphasizes how crucial it is to give people the skills and information they need to effectively control their online presence.

Social Media Platforms and Data Privacy: There is comparatively less trust in social media platforms' dedication to privacy (mean = 3.03). While some people may be suspicious, others may be more trusting, according to the significant difference between the groups (p = 0.841). This gap can be closed by enhancing social media activities' accountability and openness.

Digital Footprint Education: Participants firmly feel that educating individuals about managing their digital footprints is important (mean = 4.09). The notable difference between the groups (p = 0.694) suggests that although everyone agrees that education is necessary, opinions on apparent responsibility and priority may differ.

Privacy Advocacy: It is clear that users want more privacy protections in social media regulations (mean = 3.93). The groups' substantial difference (p = 0.049) emphasizes the necessity of active participation and advocacy from those who really believe in this digital footprint concept.

Security Concerns: Participants have major concerns about the security of their data posted on social media (mean = 3.90). The significant difference between groups (p = 0.047) suggests that the degree of concern varies among highly agreeing and disagreeing individuals. A holistic approach including technical sound mechanism and user education is needed to address these issues and overcome the same to certain expend.

Comfort and Personalized Advertising: People are generally not very comfortable with businesses using their data for personalized advertising (mean = 2.81). While some people are more receptive, others may be more concerned about their privacy, as indicated by the significant difference between the groups (p = 0.748). This emphasizes the crucial importance of transparency and user authority over data use.

Privacy as a Fundamental Right: The majority of participants (mean = 4.08) believe that privacy is a fundamental right in the digital sphere. There is broad agreement on this matter, as seen by the significant difference across groups (p = 0.923), however some people have more strongly held opinions than others. This emphasizes how crucial it is to promote strict regulations on privacy and safety protocols.

Conclusion And Recommendations-

This research shows a multifaceted correlation between individuals' online actions, privacy concerns, and their awareness of digital footprints. Though majority of respondents acknowledge the relevance of managing their digital footprint, there are notable differences in their practices, attitudes, and level of expertise.

Concerns over data security and privacy, especially with regard to social media platforms, were voiced by numerous participants. The use of default settings and a lack of knowledge about good privacy practices were understood, too. To enable people to take charge of their digital footprint, the results emphasize the necessity of thorough education and awareness initiatives.

To effectively address these challenges, the following approaches are put forth:

- For a safer online experience, we can offer customized digital education programs that can fill in specific knowledge gaps across age groups and teach people about privacy, security, and ethical digital behavior.
- Simplify privacy settings on internet services and social media platforms so that users of all ages and technical skill levels can simply access and understand them.
- Platform privacy settings should be made simpler and more uniform to foster smart privacy options and to ensure transparency and understanding for users of all ages and technical skill levels.
- Governments need to set down strong data protection regulations that encourage businesses to employ strict data security measures while imposing severe penalties for data breaches and misuse.
- To build a safer online environment and encourage knowledge and innovation in privacy and security technology, encourage cooperation between educators, tech businesses, and legislators.
- In order to improve personal security, encourage people to take proactive control of their digital footprints by examining privacy settings, creating secure passwords, and sharing information online with caution.

Reference-

Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and individual differences*, *124*, 150-159. https://doi.org/10.1016/j.paid.2017.12.018

Christian, J. (2024). Protecting Your Digital Identity: A Comprehensive Guide to Managing Your Digital Footprint. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *15*(1), 744-752.

Golder, S. A., & Macy, M. W. (2014). Digital footprints: Opportunities and challenges for online social research. *Annual review of sociology*, *40*(1), 129-152. https://doi.org/10.1146/annurev-soc-071913-043145

https://books.google.co.in/books?hl=en&lr=&id=VDU7CgAAQBAJ&oi=fnd&pg=PA354&dq=digital+footprint+social+media&ots=D1RDBwzknN&sig=QS_TaMCOs354uqDKHX33kWsBPOg&redir_esc=y#v=onepage&q=digital%20footprint%20social%20media&f=false

https://ijmlrcai.com/index.php/Journal/article/view/257/305

Kligienė, S. N. (2012). Digital footprints in the context of professional ethics. *Informatics in Education-An International Journal*, *11*(1), 65-79. https://www.ceeol.com/search/article-detail?id=195892

Micheli, M., Lutz, C., & Büchi, M. (2018). Digital footprints: an emerging dimension of digital inequality. *Journal of Information, Communication and Ethics in Society*, *16*(3), 242-251. https://doi.org/10.1108/JICES-02-2018-0014

Osborne, N., & Connelly, L. (2015, July). Managing your digital footprint: Possible implications for teaching and learning. In *Proceedings of the 2nd European Conference on Social Media ECSM* (pp. 354-361).

Weaver, S. D., & Gahegan, M. (2007). Constructing, visualizing, and analyzing a digital footprint. *Geographical Review*, *97*(3), 324-350. https://doi.org/10.1111/j.1931-0846.2007.tb00509.x