International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Analysing the Degree of Awareness of Corporate Dataveillance on Consumer Privacy

Maitreyi Singh[1], Aviral Amar[2], Bala Avijit Chaturvedula[3], Arnav Tripathi[4]

[1]Student, Department of Chemical Engineering, Birla Institute of Technology and Science, Pilani,
[2,3]Student, Department of Mechanical Engineering, Birla Institute of Technology and Science, Pilani,
[4]Student, Department of Computer Science, Birla Institute of Technology and Science, Pilani,

Abstract

With the rapid growth of digital technologies and the proliferation of data-driven services, understanding the dynamics of data privacy has become crucial. The present study explores the extent of awareness of the urban population of India in regards to corporate data surveillance on consumer privacy. It examines the degree of transparency with which corporations ask their customers for consent and the extent to which individuals are willing to share their private information. This study combines insights from diverse sources to shed light on the mechanisms by which data is gathered and shared. The findings were examined extensively using the SPSS software to ascertain the implications on user privacy in the form of quantitative analysis, based on the following parameters: technological proficiency, awareness, user perception, transparency, and regulations. By studying the factors influencing people's decisions to share personal data, this report provides a comprehensive overview of the current state of digital data privacy and its significance for individuals and businesses.

Keywords: Information security, Digital surveillance, Digital literacy, Privacy, Transparency, Regulations, Personalized advertising, Data privacy

Introduction

Data surveillance refers to the systematic monitoring, collection, and analysis of data, often with the goal of gathering information about individuals or groups [1]. There are multiple reasons for organisations to engage in data surveillance, including national security, law enforcement, and marketing. Within a business environment, the term can be narrowed down to corporate data surveillance.

Profiling, as a subset of data surveillance, is the ‘systematic and purposeful recording and classification of data related to individuals’ [2]. Algorithmic profiling refers to the practice of using algorithms to analyse and categorise data about individuals to make predictions or decisions about them. Business intelligence tools are useful in generating predictive analysis, which allows the organisation to predict likely outcomes based on past trends.

When correctly employed, BI can improve the organisation’s performance by translating collected data and refining it to enhance company marketing strategies [3]. One of these is personalised or targeted advertising, a form of online advertising that aims to deliver relevant content and advertisements to specific individuals or groups based on their characteristics, preferences, or online behaviour [4]. Data

provided by individuals can be accessed via third party applications, cookies, e-commerce cart retargeting (ECR) etc. Analytics cookies provide valuable insights into user behaviour and can help improve the user experience [5,6].

As embedded computing and the IoT have grown in popularity, data surveillance has grown more pervasive [7]. There are concerns about privacy risks and the negative impact on trust that can arise from excessive or opaque data tracking, including identity theft, financial fraud, cyberbullying, and stalking. There also exist reservations regarding the lack of transparency, which refers to the openness and clarity with which organisations communicate their practices, policies, and intentions related to the collection, monitoring, and use of data [8].

Promoting consumer awareness and education is essential for safeguarding user privacy. Certain regulations have been imposed in the field of data surveillance and online sharing of data to protect individuals and help them maintain their privacy. Some significant regulations are the Digital Data Protection Bill, 2023 in India and the General Data Protection Regulation (GDPR) in the EU [9].

Review of Literature and Hypotheses

Digital Maturity

Digital maturity is defined as the "level of technological proficiency and skills an organisation possesses by which to effectively navigate and utilise digital tools, platforms, and resources" [10]. Even though students in the current era gain exposure to digital technologies from a young age, they might not be as technologically proficient as suggested [11]. The COVID-19 pandemic brought about a need to master these skills, indicating that students have improved their proficiency levels during the pandemic [12].

With increased internet activity and digital literacy, there comes an increased threat of attacks on data privacy. People are becoming more concerned about their online privacy and are taking steps to protect it. Some strategies to protect personal information include using false names, restricting access to profiles, changing privacy settings, and ignoring friend requests from unknown people [13]. Digital thinking now involves the identification of fake news, countering misinformation, and navigating echo chambers, particularly in the heightened concerns about cybersecurity during periods of political, social, or economic upheaval, such as elections or the pandemic [14].

Impact of Transparency on User Perceptions

User perceptions of online behavioural advertising are heavily influenced by their trust in organisations and the transparency of data exchanges. Organisations must clearly communicate the extent of data use to users, as transparency builds trust and prevents irreparable damage to their reputation in case of malpractice [15]. Surveys indicate that users are more willing to share personal data with brands they trust. For example, a Harvard Business Review article found healthcare companies ranked highest in trustworthiness, while social media giants ranked lowest. It is also shown that users generally accept data collection when it enhances services, such as personalised maps or targeted marketing, as they see it as a fair trade-off. However, selling personal information to third parties demands high value in return, and users often expect significant benefits [16].

Negative perceptions arise when users feel their privacy is invaded, especially when encountering unexpected targeted ads or realising the extent of algorithmic profiling. This disillusionment can be exacerbated by a lack of understanding of how data is used, leading to emotional and cognitive reactions like surprise and disbelief [17,18]. Trust issues are prevalent, as nearly half of Americans find it unacceptable for social media companies to analyse user behaviour for personalised content, and many

distrust these companies regarding data misuse [19]. Users are particularly concerned about the security of children's information and the potential misuse of data by online platforms.

To achieve greater transparency, companies must educate consumers about data utilisation, seek permission before use, and provide tangible value in return. However, persistent issues like "consent fatigue" can undermine these efforts, as users may hastily click through cookie banners without fully understanding their choices [20,21]. Despite global legislation aimed at curbing data mining, many websites still lack transparency about cookie use, with only 14% of investigated sites not setting non-essential cookies without consent [5]. Companies must prioritise privacy by design, incorporate security measures from the outset, and ensure clear, accessible opt-out options to maintain user trust and compliance with data protection standards.

Objective

This research paper aims to critically analyse the extent of awareness among consumers regarding corporate data surveillance practices, and explore the impact of personalised advertising strategies on perceptions of privacy. Our study encompasses participants from different demographics, including gender, household income, and age group, to provide a comprehensive understanding of these topics. The hypotheses are based on five dimensions: technological proficiency, awareness of data collection and its extent, user perceptions regarding the quality of search, apprehension regarding transparency exhibited by organizations, and knowledge about regulations imposed by the government.

Historically, there has been a stereotype that men are more digitally competent than women. As men were more likely to have access to technology and education in the past, it was assumed that women would take longer to catch up to men. A study conducted by BlockSurvey extended this hypothesis with their findings. Men tend to use VPNs more than women, along with email encryption programs, password managers, privacy-enhancing browsers and search engines, and two-factor authentication. This portrayed women as less aware of the availability of privacy tools than men [22].

Men are also known to dominate technology development. According to a study, there was a stark contrast in career expectations between men and women, with only 1% of women envisioned working in ICT fields as compared to 10% of men. Fewer female students opt to enrol in STEM studies, leading to a great gender imbalance in STEM fields such as ICT [23]. Hence, the following hypothesis is proposed.

H1: Men will result in higher mean scores than women for most dimensions, namely a) technological privacy, b) awareness, c) transparency, and d) regulations.

Young people have grown up in an era where technology is ubiquitous and digital devices are a part of daily life. However, they often exhibit a degree of naivety when it comes to digital security, and are not as proficient with technology as expected [11]. Early adolescents do not find risks about corporations and data collection practices as alarming as risks associated with potential online predators [24]. We may be able to extend this finding to young adults as well.

Older adults, having been exposed to technology throughout their professional lives, may also exhibit greater caution and awareness as compared to younger individuals who have grown up with technology. Although it is difficult to assume anything about technological proficiency, we can make the following hypothesis based on these arguments.

H2: Individuals aged 25-60 will have higher mean scores than those aged 18-25 and 18+ in the dimensions of a) awareness, b) transparency, and c) regulations.

We will form three major income brackets, i.e. < Rs 5 lakhs, Rs 5-12 lakhs, and > Rs 12 lakhs, to stipulate our final hypothesis. Individuals earning more than Rs five lakhs are typically engaged in white-collar

jobs. These jobs require an office setting and the work is generally computer-oriented [25]. Due to regular internet interaction, they may also attempt to safeguard themselves against unethical practices. We can now stipulate our final hypothesis.

H3: Individuals in the lower income brackets (< Rs 5 lakhs and Rs 5-12 lakhs) demonstrate lower mean scores than those in the higher income bracket (> Rs 12 lakhs) in the areas of a) technological proficiency, b) awareness, c) transparency, and d) transparency.

Methodology

Research Design

For the collection of primary data, we collected answers to our questionnaires from different groups of people who were divided on the basis of age groups, gender and income. In order to make answering the survey easier for respondents, we made all the questions on a 5 point Likert scale. The identity of respondents remained anonymous as we did not ask for name or phone number, Aadhar number etc. To ensure authenticity of the data collected we only circulated the questionnaire among trusted family and friends.

A diverse set of people of both genders from different age groups and economic backgrounds were approached for this survey, making the research representative and inclusive. The Google Form was open for 3 days and a total of 192 responses were collected out of which 189 were authentic. Table 1 provides demographic information of the respondents.

TABLE I. DEMOGRAPHICS

Variable		Number of Respondents	Percentage
Gender	Male	125	66.14%
	Female	64	33.86%
Age Group	< 18 years	11	5.79%
	18 - 25 years	53	27.89%
	25 - 60 years	124	65.26%
	> 60 years	2	1.05%
Household Income	< Rs 5 lakhs	21	11.11%
	Rs 5 - 12 lakhs	51	26.98%
	> Rs 12 lakhs	117	61.91%

Research Instruments

An online questionnaire containing two different parts was circulated. The first recorded the demographic information of the respondents (displayed in Table 1), while the second part contained 17 questions based on our study in a 5-point Likert scale. The options ranged from 1-5: (1) Strongly Disagree, (2) Slightly Disagree, (3) Neutral, (4) Slightly Agree, (5) Strongly Agree. The questions were divided into 5

dimensions as stated above: technological proficiency, awareness, user perception, transparency, and regulations.

Statistical Analysis Methods

Once we collected the data, we processed it using the SPSS Statistics software developed by IBM. As we were interested in determining whether there were statistically significant differences in the mean, we used Independent Samples t-testing and ANOVA. The Games-Howell post-hoc test was also conducted where the assumption of equal sample sizes was violated. We analysed the results to validate our hypotheses.

Results

We tested all different possible combinations of variables and demographics. Due to limitations in space, we will only display the results where there was a statistically significant difference in the mean scores. We produced six results and have displayed them in the form of tables. Table 2 to Table 7 show the information regarding the mean scores and have been listed as the combination of a dimension and variable. The results shall be discussed in the upcoming section. Due to the lack of respondents of the age group < 18 years and > 60 years, we have omitted those results.

Mean Scores

TABLE II. TRANSPARENCY: GENDER

Gender	N	Mean	Std. Deviation	Std. Error Mean
Male	121	3.7438	0.47062	0.04278
Female	62	3.4823	0.44410	0.05640

TABLE III. TECHNOLOGICAL PROFICIENCY: INCOME

Income	N	Mean	Std. Deviation	Std. Error Mean
< Rs 5 lakhs	20	4.0340	0.96643	0.21610
> Rs 12 lakhs	116	4.3369	0.69627	0.06465

TABLE IV. AWARENESS: INCOME

Income	N	Mean	Std. Deviation	Std. Error
< Rs 5 lakhs	20	3.4995	1.16772	0.26111
Rs 5 - 12 lakhs	50	3.4998	0.90383	0.12782
> Rs 12 lakhs	116	3.0587	1.02073	0.09477

TABLE V. TRANSPARENCY: INCOME

Income	N	Mean	Std. Deviation	Std. Error
< Rs 5 lakhs	20	3.5500	0.52265	0.11687
Rs 5 - 12 lakhs	49	3.5000	0.48132	0.06876
> Rs 12 lakhs	114	3.7404	0.44993	0.04214

TABLE VI. REGULATIONS: INCOME

Income	N	Mean	Std. Deviation	Std. Error
< Rs 5 lakhs	20	3.9250	1.13873	0.25463
Rs 5 - 12 lakhs	44	3.4830	0.73413	0.11067
> Rs 12 lakhs	114	3.1689	0.86570	0.08108

TABLE VII. REGULATIONS: AGE

Age	N	Mean	Std. Deviation	Std. Error Mean
18 - 25 years	49	2.8520	0.81637	0.11662
25 - 60 years	116	3.5576	0.84790	0.07873

Significance Testing

An independent t-test (also known as an independent samples t-test or two-sample t-test) is a statistical test used to determine whether there is a significant difference between the means of two independent (unrelated) groups.

ANOVA (Analysis of Variance) is a statistical technique used to determine if there are significant differences between the means of three or more independent groups. It extends the t-test to multiple groups, allowing for comparisons across more than two groups simultaneously. In order to determine significant differences, we calculate the one-tailed p-value and compare it to the significance level, α, which we have taken as 0.05. If the p-value < α, we can interpret that there is a statistically significant differences in mean scores, and that there is a very low chance that the values are random.

Sometimes the sample sizes of different variables vast greatly, violating the assumption of equal sample sizes. In these cases, we can use the Games-Howell post-hoc test after performing an ANOVA.

Table 8 depicts whether the tests gave statistically significant differences.

Hypothesis	Variable	Dimension	P-Value	Significant Difference
H1	Gender	Technological Proficiency	0.422	No
		Awareness	0.288	No

		Transparency	< 0.001	Yes
		Regulations	0.111	No
H2	Age Group	Awareness	0.072	No
		Transparency	> 0.7	No
		Regulations	< 0.001	Yes
H3	Income Bracket	Technological Proficiency	0.047**	Yes
		Awareness	0.018*	Yes
		Transparency	0.010*	Yes
		Regulations	0.025**	Yes

*Income Bracket: 5 – 12, > 12 lakhs
**Income bracket: < 5, > 12 lakhs

Discussion

Beginning with H1, we can see that only one dimension, transparency, produces statistically significant differences in the mean scores. As per Table 2, males score a mean of 3.74 while females score 3.48. The result aligns with our hypothesis H1.c. As stated earlier, more men tend to be part of STEM and ICT fields as compared to women [23]. The other subparts of H1 could not produce any significant result but the mean score of women (4.27) was much higher than we expected. In fact, it was exactly equal to that of men! While we cannot predict anything from these results as they could be random, there could be a few reasons for this outcome.

The COVID-19 pandemic triggered significant changes across various domains and one of the notable transformations was in the realm of technology use. With the necessity for social distancing and lockdowns, there was a widespread shift to online learning for children and remote work for professionals. This sudden and widespread adoption of digital platforms led to a substantial improvement in technological skills within a relatively short time frame. It extended to men and women alike, which could be one of the ways of bridging the gap.

Contrary to our findings, a report from the Metropolitan Policy Program at the Brookings Institution, “Digitalization and the American Workforce”, mentioned that women were more apt for high-tech jobs, giving them a digital score of 48 instead of 45 for men [26].

For working females, the adaptation to remote work brought about a reliance on virtual meetings and the need to employ new and diverse techniques to carry out their tasks efficiently. As traditional offices gave way to remote setups, women in the workforce navigated a digital landscape where effective communication and collaboration became paramount. The challenges posed by this shift compelled individuals to explore and master various digital tools and platforms, fostering a quicker acquisition of technological skills.

While we cannot be certain that these are the reasons or that the score implies anything due to a high p-value, it gives us the possibility to do some research on this topic in the future.

Coming to our next hypothesis, H2, there was only one dimension (regulations) that produced the result we predicted. Table 7 showed that the mean for individuals in the age group 18 – 25 years scored a lower mean (2.85) than those of the age group 25 – 60 years (3.56). Once again, our hypothesis has proven correct but only for H2.c.

A study was conducted to find out early adolescents' perspective on digital privacy, using a sample of youth aged 11-14. An important distinction in their perspective is based on the two different categories of privacy – proximal and distal. The needs of intimacy, affiliation, exploration, and information control that are rooted in daily relationships, peer groups, and families are all part of adolescents' proximal, person-to-peer privacy management [27]. For instance, teenagers' discomfort with uninvited parties viewing their personal information frequently influences their attitudes toward online privacy and safety [28].

On the other hand, distal privacy involves a better understanding of how businesses and data brokers gather and exchange personal information is necessary for distal privacy management. Adolescents' person-to-corporation privacy management may present difficulties for tweens, who are only starting to think abstractly and comprehend social issues. In addition, adolescents may be less alarmed by impersonal invasions of privacy by law enforcement, businesses, or governments than by the more direct threats of inquisitive parents or classmates [28].

The key findings that were published indicated that adolescents reported more proximal than distal privacy protection behaviours. Though this study was conducted on adolescents, it is possible to extend the argument to young adults.

Our final hypothesis, H3, produced statistically significant results for all the dimensions that we tested. Tables 3 to 6 can be referred to for mean scores. Regarding technological proficiency and transparency, our hypotheses proved to be correct. Individuals belonging to a higher income bracket did score a higher mean than those belonging to the lower income brackets.

As mentioned before, most individuals in the higher income bracket work white-collar jobs and are accustomed to working with computers, hence H3.a. Employees tend to realise that they are accountable for maintaining the confidentiality and integrity of digital information entrusted to them. Specific workplace cultures that prioritise transparency, accountability, and ethical behaviour tend to place a strong emphasis on digital privacy guidelines.

Many organisations conduct regular training sessions or workshops to educate employees about digital privacy regulations, the importance of data protection, and best practices for safeguarding personal information. Employees may be given a handbook including information about digital privacy regulations. This serves as a reference guide for employees to understand their rights and responsibilities regarding data privacy.

The Privacy Due Diligence (PDD) model, which is customised to specific business models and workplace environments, is an organised method for managing privacy issues in the workplace as a continuous practice. The PDD model integrates insights from privacy and human behaviour analytics literature with the standards for human rights due diligence specified in the UN Guiding Principles on Business and Human Rights (UNGPs) [29]. The PDD model follows a four-step logic:

Mapping the 'privacy footprint': This step involves identifying and understanding the scope and impact of data collection, processing, and storage activities on employee privacy within the organisation.

Privacy gap analysis: This entails assessing any gaps or shortcomings in current privacy protection measures and practices.

Setting priorities for management, impact reduction, and measures: Identifying the most important areas for improvement, putting privacy gaps into action, and controlling how these actions affect employee privacy.

Establishing procedures and systems to guarantee continuous privacy protection, incorporating essential components of employment and data protection laws, and enlisting the help of outside parties to fortify privacy practices are all ways to "anchor" privacy protection at work.

However, it was surprising that while such a model exists to familiarise employees with data protection laws and regulations, it was individuals from the lower income brackets who scored higher in terms of awareness and regulations. Several explanations could exist for this phenomenon.

While the initial assumption may have held true in the pre-COVID era, the pandemic has significantly altered the job landscape in India. Lockdowns necessitated remote work, leading to increased technological and internet proficiency among employees during this period.

Government initiatives, such as upskilling programs like Skill India or Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA), have been in place for several years [30]. These programs focus on promoting digital literacy in rural areas, including those from marginalised and economically disadvantaged backgrounds. They offer free online courses to bridge the knowledge gap. These initiatives were especially helpful during the COVID-induced lockdown as the increased availability of spare time contributed to this awareness.

The reliance on digital services is also a factor. Individuals with lower incomes heavily depend on digital services for communication, information access, and employment opportunities. Consequently, they may be more conscious of the rules governing these services to actively participate in the digital economy.

Government assistance programs often require online applications and communication. Individuals with lower incomes must be well-versed in digital rules and regulations to navigate these processes successfully and receive the necessary support.

The level of disposable income plays a role in this phenomenon. With lower incomes, individuals tend to be more cautious about various threats, leading to increased awareness of rules and regulations.

Conclusion

The results of this study affirm the initial hypotheses various demographics, with some notable exceptions. Gender-based analysis showed that men exhibited greater confidence and attitudes toward digital skills and ICT, aligning with the hypothesis that men would score higher in technological proficiency and awareness of data collection. This reflects the influence of historical factors on gender attitudes towards technology.

Age group analysis demonstrated that individuals aged 25-60 scored higher in awareness of data collection, apprehension regarding organizational transparency, and knowledge about regulations, consistent with our hypothesis. This demographic's exposure to technology in professional settings, rather than being born into it, likely contributes to their increased caution and understanding of data privacy issues.

However, the income level analysis produced mixed results. As expected, individuals with lower incomes had lower scores in technological proficiency and transparency, likely due to less access to technology. Contrary to our hypothesis, they exhibited higher scores in awareness of data collection and knowledge about regulations. This indicates that lower-income individuals may be more cautious and informed about data privacy issues, possibly due to heightened apprehension about potential misuse of their data. These

findings highlight the complex relationship between socioeconomic factors and digital competence, emphasizing the need for nuanced approaches to digital education and policy-making.

References

1. M. Büchi, E. Fosch-Villaronga, C. Lutz, A. Tamò-Larrieux, and S. Velidi, "Making sense of algorithmic profiling: user perceptions on Facebook," *Information, Communication & Society*, vol. 26, no. 4, pp. 1–17, Oct. 2021, doi: https://doi.org/10.1080/1369118x.2021.1989011.
2. R. Clarke and G. Greenleaf, "Dataveillance Regulation: A Research Framework," *Social Science Research Network*, Jan. 2017, doi: https://doi.org/10.2139/ssrn.3073492.
3. "Business Intelligence in Marketing Explained | Impact Networking," *Impactmybiz.com*, 2021. https://www.impactmybiz.com/blog/business-intelligence-marketing-explained/ (accessed Apr. 24, 2024).
4. K. Donlan, "What Is Personalized Marketing? Strategy, Examples & Trends," *Emarsys*, Mar. 03, 2023. https://emarsys.com/learn/blog/what-is-personalized-marketing/ (accessed Sep. 17, 2023).
5. Benjamin Maximilian Berens, M. Bohlender, H. Dietmann, and M. Volkamer, "Cookie Disclaimers: Dark Patterns and Lack of Transparency," *ResearchGate*, Sep. 2023. https://www.researchgate.net/publication/374244568_Cookie_Disclaimers_Dark_Patterns_and_Lack_of_Transparency (accessed Nov. 14, 2023).
6. L. Xueming, "The Double-Edged Effects of E-Commerce Cart Retargeting: Does Retargeting Too Early Backfire? - Jing Li, Xueming Luo, Xianghua Lu, Takeshi Moriguchi, 2021," *Journal of Marketing*, 2021. https://journals.sagepub.com/doi/10.1177/0022242920959043
7. U. Gal, "Data surveillance is all around us, and it's going to change our behaviour," *Apo.org.au*, Oct. 11, 2016. https://apo.org.au/node/68257
8. S. McPherson, "What is Data Transparency?," *Melissa.com*, Nov. 13, 2023. https://knowledge.melissa.com/en-gb/what-is-data-transparency
9. "The Digital Personal Data Protection Bill, 2023," *PRS Legislative Research*. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
10. A. Rossmann, "Digital Maturity: Conceptualization and Measurement Model," *ResearchGate*, 2019. https://www.researchgate.net/publication/345760193_Digital_Maturity_Conceptualization_and_Measurement_Model
11. Julio Cabero Almenara, Francisco David Guillen-Gamez, J. Ruiz-Palmero, and A. Palacios-Rodríguez, "Teachers' digital competence to assist students with functional diversity: Identification of factors...," *ResearchGate*, Jan. 13, 2022. https://www.researchgate.net/publication/353732661_Teachers%27_digital_competence_to_assist_students_with_functional_diversity_Identification_of_factors_through_logistic_regression_methods
12. Marcin Awdziej, M. Jaciow, M. Lipowski, and R. Wolny, "Students Digital Maturity and Its Implications for Sustainable Behavior," *ResearchGate*, Apr. 27, 2023. https://www.researchgate.net/publication/370322951_Students_Digital_Maturity_and_Its_Implications_for_Sustainable_Behavior
13. Spyros Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *ResearchGate*, Jul. 10, 2015. https://www.researchgate.net/publication/280244291_Privacy_attitudes_and_privacy_behaviour_A_review_of_current_research_on_the_privacy_paradox_phenomenon

14. B. Puig, Paloma Blanco-Anaya, and J. J. Pérez-Maceira, "'Fake News' or Real Science? Critical Thinking to Assess Information on COVID-19," *Frontiers in education*, vol. 6, May 2021, doi: https://doi.org/10.3389/feduc.2021.646909.
15. "Data-driven digital advertising: benefits and risks of online behavioral advertising | Emerald Insight," *International Journal of Retail & Distribution Management*, vol. 49, no. 7, pp. 1089–1110, 2020, doi: https://doi.org/10.1108//IJRDM.
16. "Customer Data: Designing for Transparency and Trust," *Harvard Business Review*, May 2015. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust
17. S. Hautea, Anjali Munasinghe, and E. Rader, "'That's Not Me': Surprising Algorithmic Inferences," *ResearchGate*, Apr. 25, 2020. https://www.researchgate.net/publication/341722400_'That's_Not_Me'_Surprising_Algorithmic_Inferences
18. M. A. de, Somaya Ben Allouch, and J. A.G.M, "Why Do They Refuse to Use My Robot?: Reasons for Non-Use Derived from a Long-Term Home Study," *ResearchGate*, Mar. 2017. https://www.researchgate.net/publication/312654128_Why_Do_They_Refuse_to_Use_My_Robot_Reasons_for_Non-Use_Derived_from_a_Long-Term_Home_Study
19. S. Atske, "How Americans View Data Privacy," *Pew Research Center*, Oct. 18, 2023. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/
20. H. Choi, J. Park, and Y. Jung, "The role of privacy fatigue in online privacy behavior," *Computers in human behavior*, vol. 81, pp. 42–51, Apr. 2018, doi: https://doi.org/10.1016/j.chb.2017.12.001.
21. C. Utz, M. Degeling, S. Fahl, and T. Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field," *ResearchGate*, Nov. 11, 2019. https://www.researchgate.net/publication/334965379_Uninformed_Consent_Studying_GDPR_Consent_Notices_in_the_Field
22. Harini Anantha Rajan, "Are people aware of Digital Privacy? - BlockSurvey - Medium," *Medium*, Jan. 06, 2020. https://medium.com/blocksurvey/are-people-aware-of-digital-privacy-ad8d7341c3ff
23. "Men dominate technology development," *European Institute for Gender Equality*, Feb. 2021. https://eige.europa.eu/publications-resources/toolkits-guides/gender-equality-index-2020-report/men-dominate-technology-development?language_content_entity=en
24. N. D. Santer, A. Manago, A. Starks, and S. M. Reich, "Early Adolescents' Perspectives on Digital Privacy," *Works in Progress*, Jun. 29, 2021. https://wip.mitpress.mit.edu/pub/early-adolescents-perspectives-on-digital-privacy/release/1
25. J. Gillis, "20 Best White-Collar Jobs," *The Interview Guys - Job Interview Prep, Interview Questions & Career Advice*, Mar. 2021. https://theinterviewguys.com/white-collar-jobs/
26. J. Whiton, M. Muro, S. Kulkarni, and S. Liu, "Digitalization and the American workforce," *Brookings*, Nov. 15, 2017. https://www.brookings.edu/articles/digitalization-and-the-american-workforce/
27. P. M. Valkenburg and J. Peter, "Adolescents' Online Privacy: Toward a Developmental Perspective," *ResearchGate*, Jun. 19, 2011. https://www.researchgate.net/publication/279190144_Adolescents'_Online_Privacy_Toward_a_Developmental_Perspective
28. N. D. Santer, A. Manago, A. Starks, and S. M. Reich, "Early Adolescents' Perspectives on Digital Privacy," *Works in Progress*, Jun. 29, 2021. https://wip.mitpress.mit.edu/pub/early-adolescents-perspectives-on-digital-privacy/release/1 (accessed Jun. 30, 2024).

29. Isabel Laura Ebert, I. Wildhaber, and Jeremias Adams-Prassl, "Big Data in the workplace: Privacy Due Diligence as a human rights-based approach to employee privacy...," *ResearchGate*, May 2021. https://www.researchgate.net/publication/351447441_Big_Data_in_the_workplace_Privacy_Due_Diligence_as_a_human_rights-based_approach_to_employee_privacy_protection (accessed Jun. 30, 2024).
30. "Pradhan Mantri Gramin Digital Saksharta Abhiyaan," *myScheme - One-stop search and discovery platform of the Government schemes*, 2024. https://www.myscheme.gov.in/schemes/pmgdisha