Compromising Privacy: The Role of AI in Smartphone Surveillance

Md Absarul Hasan

Senior Journalist, DD News, India’s Public Service Broadcaster

Abstract:
In the contemporary digital landscape, smartphones have evolved into essential devices, seamlessly integrating into everyday life to facilitate communication, information access, and numerous tasks. However, their omnipresence has also paved the way for an era of pervasive surveillance. Both governmental bodies and technology corporations have increasingly exploited these devices to monitor and gather data from users, often without clear consent. The integration of Artificial Intelligence (AI) with mobile technology has further intensified surveillance capabilities, establishing a system that is omnipresent yet largely invisible. Cases, such as Uber being fined by the Dutch Data Protection Authority, Meta admitting to censoring Covid-19 data in the U.S. under pressure from the White House and fine imposed by South Korea social media watchdog on Meta are clear examples of compromises in the protection of users’ personal data and the suppression of free expression.
In light of the emerging scenario driven by AI applications, this paper explores the widespread nature of smartphone surveillance, primarily because we are mostly connected to these apps through our smartphones, the critical role AI plays in advancing these practices, and the profound implications for individual privacy, autonomy, and societal norms. Through this examination, the paper sheds light on the growing complexities of digital surveillance and calls for urgent discourse on privacy and ethical considerations in the age of AI.

Keywords: Smartphone, Mobile, Artificial Intelligence (AI), Surveillance, Privacy & Ethics.

Introduction:

We are living under the shadow of “Surveillance Capitalism” (Zuboff, 2020), where we sacrifice our personal data for free services and agree to the terms and conditions of social media giants, from which surveillance begins and extends even into our private spaces. Even when the lights are off in the bedroom, the smartphone continues to monitor us, persistently sending signals about our whereabouts to numerous companies and establishments through the various applications we engage with. Mobile devices are equipped with various sensors and capabilities, such as GPS for location tracking, cameras, microphones, and accelerometers that continuously generate data. They continuously transmit location data through GPS, Wi-Fi, and cell towers. And, the advent of and use of Artificial Intelligence (AI) and biometric tools have complicated this landscape, raising concerns regarding consent, data control, and the preservation of anonymity. Applications often request access to this data, ostensibly to enhance user experience, but it can be exploited for profiling and tracking user movements in real-time. AI algorithms analyze this data to monitor user behavior, predict future actions, and identify patterns that might pose security threats or influence consumer preferences. This data is collected by mobile apps, operating systems, and even embedded firmware, often without the user's explicit consent. The €290 million fine imposed on Uber for illegally transferring European drivers' personal data to the U.S. government agencies is a recent example of the misuse of AI by the company (Khalil, 2024). In this case, Uber transferred ID documents and location information to the U.S. The Dutch Data Protection Authority stated that this violated the EU's strict data privacy rules, known as GDPR, because Uber failed to protect the data properly. This was not the first time that Uber was fined in EU. This was third fine in a series. In 2023, DPA imposed fine of €10 million, while €600,000 in 2018 for data related violation. Irish regulator fined TikTok €345 million for violating children's privacy under GDPR rules. This demonstrates that EU regulators are steadfast in enforcing the rules and are not allowing companies to evade punishment. This paper explores the future consequences of AI-driven data collection, as seen in the cases of Uber and Facebook, both of which have admitted to sharing data with America's National Security Agency (NSA). These admissions raise concerns that these companies are not only sharing data with government agencies but also potentially trading it for their benefit.

Methodology

Since the proposed study addresses an emerging phenomenon, a review of relevant literature, including published papers, case studies, and research reports, was conducted. The literature review provided insights into the trends emerging with respect to AI in mobile surveillance.

A survey was conducted in New Delhi to examine attitudes and behaviors regarding the integration of artificial intelligence (AI) in smartphones, focusing on user awareness, data privacy concerns, and personal comfort levels. Data were collected through an online questionnaire. Responses were gathered from a diverse demographic, spanning various age groups, professions, and education levels. Key areas of interest included AI-enabled smartphone features, personal privacy, data protection practices, and support for stronger regulations.

Reviews of Literature

Government Oversight on Internet Freedom

The Internet can be described as free media, yet it remains subject to government surveillance (Stewart, Lawrence & Manvell, 2012). Bolin (2018) argues that in the global media landscape, both the state and corporations have benefited from the technological advancements of the Internet, as their ultimate goal is to detect and identify digital consumers. It is our disillusionment to believe that privacy is private, as privacy policies have effectively become surveillance policies (Zuboff, 2020). AI-powered mobile surveillance systems can process vast amounts of data in real-time. For example, facial recognition technology integrated into smartphones can be used by law enforcement agencies to identify individuals in crowds. As facial recognition technology processes data rapidly with 6G internet speeds, enforcement agencies are exploiting this to curb freedom of assembly by any means necessary. Reporters Without Borders (2013) released a 'Special Report on Internet Surveillance,' identifying five countries as spy nations and five corporations as "Enemies of the Internet." These countries-Syria, China, Iran, Bahrain, and Vietnam, are noted for systematic surveillance through the internet against dissent, while corporations like Gamma, Trovicor, Hacking Team, Amesys, and Blue Coat are termed "digital era mercenaries" for selling products used by authoritarian governments to curtail rights and freedoms. China, too, has been seen as a great wall against internet freedom. Lee, Liu & Li (2012) argue that due to harsh regulations and internet policies, Google's search engine ceased its services in China in 2010. Other Google services are also restricted in the mainland. China's Electronic Great Wall plays a crucial role in blocking major social media platforms within its borders, although many people circumvent the block to access them. Iran, similarly, has complex rules for internet access and has elevated online surveillance to a new level. Iranian officials have discussed launching the “Halal Internet” (Reardon 2012) to promote cybersecurity and Islamic moral values, a project that has yet to materialize and has faced widespread criticism for restricting freedom and stifling citizens’ voices online.

Governments and corporations are increasingly using AI and mobile technology to conduct surveillance. Governments may employ AI to monitor citizens’ activities for national security purposes, while corporations might use AI to track consumer behavior and preferences. The line between security and privacy is often blurred, with AI-enhanced mobile surveillance raising concerns about the erosion of civil liberties and the potential for mass surveillance. The use of AI-driven facial recognition will severely be impacting on freedom of individual in all walks of life. The case of surveillance has proven in the case of Edward Snowden’s revelations of the National Security Agency’s (NSA) mass surveillance programs. The American agency NSA collected data from U.S. Internet companies and much of data were collected outside of the U.S. legal ambit to avoid legal challenges in the country with the cooperation from Five Eyes Intelligence Alliance (United States, the United Kingdom, Canada, Australia and New Zealand).

Recent significant development is the revelation by Meta CEO Mark Zuckerberg, who expressed regret for yielding to what he described as pressure from the U.S. government to censor certain Covid-19 content on Facebook and Instagram during the pandemic (Sweney, 2024). This is a clear example of government surveillance in the digital age, with AI playing a crucial role in collection and segregating data for urgent use by spy agencies. According to Zuckerberg, officials from the Biden administration repeatedly pressured Meta to censor posts, including humor and satire, about Covid-19 in 2021. He stated that Meta faced significant frustration from the White House when they didn't comply with these demands. Zuckerberg acknowledged that, in hindsight, some of the decisions made during that time would not be repeated and emphasized that Meta should not have compromised its content standards due to government pressure. Individuals who share their personal data now find it difficult to trust companies that have numerous examples of sharing data with government agencies to maintain their business interests. Meta had already compromised the personal data of Facebook users in the Cambridge Analytica scandal.

Privacy Risks and Ethical Dilemmas in AI-Driven Smartphone Data Collection

The constant surveillance enabled by smartphones represents a significant threat to privacy. Users often consent to data collection without fully understanding the extent or consequences of their actions. This lack of transparency is exacerbated by complex terms of service agreements and the widespread use of data aggregation practices that can de-anonymize information, leading to insight into personal lives can be invasive and manipulative (Sipior, 2014). Companies like Google, Apple, and Facebook have built business models around data collection. By monitoring user behavior through their operating systems, applications, and services, they gather vast amounts of data. This information is used for targeted advertising, which can influence consumer behavior and even political opinions. Almost every application we use requests permissions, some are essential for the app's functionality, while others are excessive and allow for the collection of personal data that can be shared or sold to third parties. In the Cambridge Analytica case, 87 million users of Facebook fell prey (Fiegerman, 2018) to this consent. The data were exposed without the consent of Facebook users. A personality quiz named ‘thisismydigitallife’, Facebook users could take up (Prokop, 2019) to participate while giving consent to their and their friends’ Facebook profiles. In this data leak, 270,000 individuals took the quiz, which later multiplied to over 50 million users, leading to the exposure of their data. Facebook later acknowledged that 87 million users' data were exposed due to the quiz competition by a third party (Confessore, 2018). This data was then utilized to create personality profiles for millions of American voters, enabling the targeting of customized political messaging for Donald Trump in the 2016 US presidential election. Data collected through smartphones can be used to reinforce societal inequalities. For example, predictive policing algorithms that rely on data from smartphones have been criticized for perpetuating racial biases. Similarly, financial institutions may use behavioral data to make decisions that disproportionately affect marginalized groups (Eubanks, 2018). The constant connectivity and awareness of being surveilled can lead to increased stress and anxiety. The pressure to maintain a certain image online, combined with the lack of privacy, can contribute to mental health issues (Turkle, 2015). The recent fine levied on Facebook by South Korea highlights one of the largest cases of data collection and misuse by the social media giant. Reports indicate that Facebook collected sensitive user information without obtaining proper consent and subsequently sold this data to advertisers. This practice underscores a growing trend where companies use AI-integrated smartphones to gather vast amounts of user data, often without transparent consent. This case raises significant concerns about the extent of data collection by social media platforms, highlighting a pressing need for stronger regulatory safeguards to protect user privacy and ensure responsible data usage. The integration of AI with mobile surveillance technologies poses significant ethical challenges. The collection and analysis of personal data without user consent, the potential for discrimination through biased AI algorithms, and the psychological effects of constant surveillance are critical issues that need to be addressed. Privacy laws and regulations are struggling to keep pace with the rapid advancements in AI and mobile technology, leading to a growing debate about the need for stronger data protection measures (Mishra, 2024).

Chilling Effect on Free Speech

The knowledge that one's communications and actions are being monitored can stifle free expression. Individuals may avoid discussing controversial topics or engaging in activism due to fears of surveillance and potential repercussions (Penney, 2016) "because even the best information security programs are not 100% guaranteed to protect personal information online" (Thomson Reuters, n.d.). The knowledge that one is constantly being watched can lead to self-censorship and a reduction in the freedom to explore ideas and behaviors outside societal norms. Arun (2019) stressed that if conversations are leaked or shared with government agencies, it could result in a chilling effect on human rights. As surveillance becomes an accepted part of daily life, resistance to it diminishes. This normalization can lead to the erosion of civil liberties and the acceptance of invasive technologies in other areas of life (Ball et al., 2012). This also leads to creation of anonymous account online to resist surveillance, including the use of masks to counter facial recognition systems in public life (Purdy, 2015). And this trend has been observed online as millions of social media accounts are anonymous but the tech giants are not filtering it because of their constraints of losing the viewership's online.

Key Findings of the Survey

1. Demographics and Familiarity with AI:

Age groups varied, with respondents spanning from "Under 18" to "45 and above." Professions included students, government and private sectors employees, journalists, homemakers, and others, with education levels from "High School" to "Doctorate."

Familiarity with AI was generally high, with many respondents describing themselves as 'very familiar' or 'somewhat familiar' with AI technologies. Nearly 60% of respondents held a postgraduate degree.

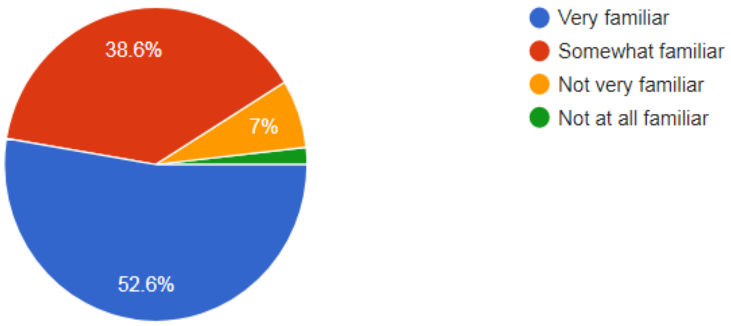

Fig.1

52.6% of respondents described themselves as 'very familiar' with AI, while 38% said they were 'somewhat familiar.' Only 3.5% of respondents with an education level below high school reported being unaware of AI integration in smartphones.

2. Frequency of AI Feature Use:

Respondents reported varying frequencies of using AI features such as virtual assistants, face recognition, and personalized recommendations. While some used these features daily, others interacted with them only occasionally or a few times a week. Specifically, 35.1% of respondents used AI assistance features on their smartphones daily, 17.5% used them a few times a week, 33.3% used them occasionally, and 14% did not use them at all.

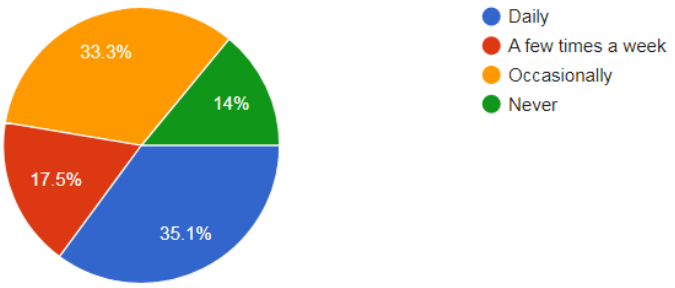

Fig.2

3. Awareness and Privacy Concerns:

The majority of respondents were aware of AI's role in data collection through smartphone applications, with 68.4% being fully aware of data collection from their smartphones.

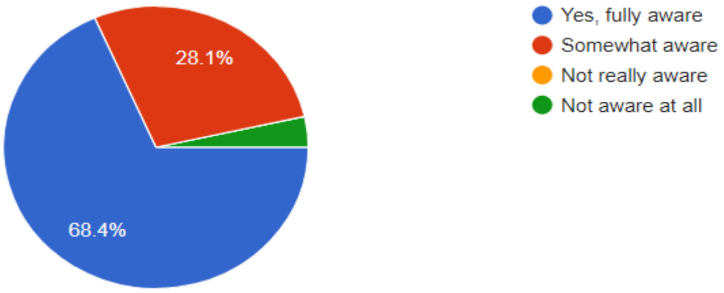

Fig.3

Concerns about personal privacy due to AI in smartphones were prominent, with many respondents feeling that AI impacts their privacy 'a great deal.' Specifically, 61.4% expressed the highest level of concern about data being collected from their smartphones by mobile applications.

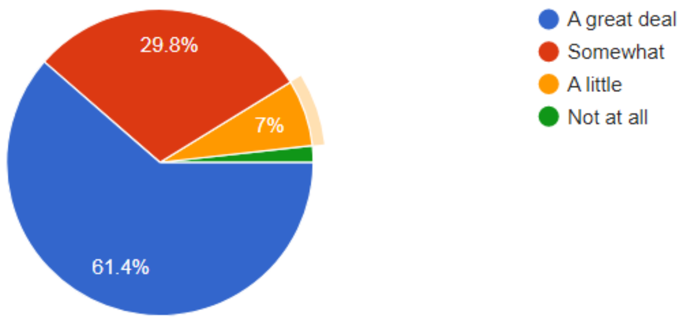

Fig.4

4. Data Collection and App Permissions:

Most participants expressed concern over the amount of personal data collected by AI features in their smartphones. They also reported feeling uncomfortable about extensive data access requested by apps.

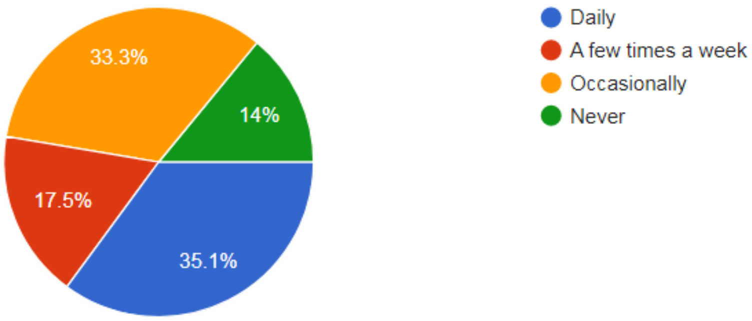

Fig.5

5. Perceived Monitoring and Privacy Laws:

Many respondents believe that smartphone AI features may monitor their activities even when not actively in use, with 63.2% expressing anxiety about frequent monitoring of their mobile data."

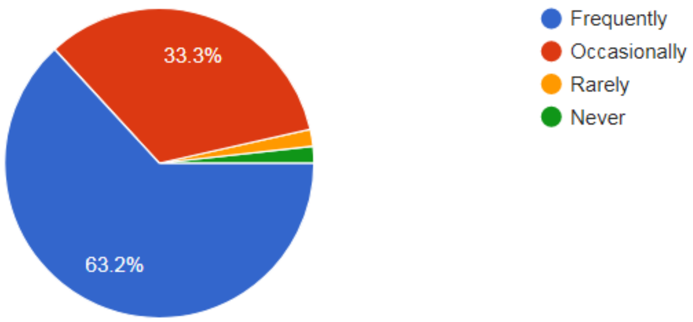

Fig.6.

6. Behavioral Responses to Privacy Concerns:

Most respondents admitted to rarely or only occasionally reading app privacy policies before installation, with only 5% reporting that they always read the privacy policy.

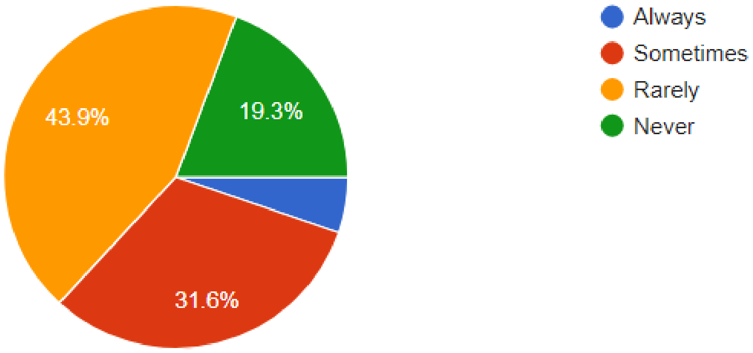

Fig.7

When made aware of excessive data collection, many indicated they would likely stop using such apps, with responses ranging from 'Probably' to 'Definitely.' 64.9% said they would stop using the app if it was found to be collecting excessive data and would definitely delete the app from their mobile devices.

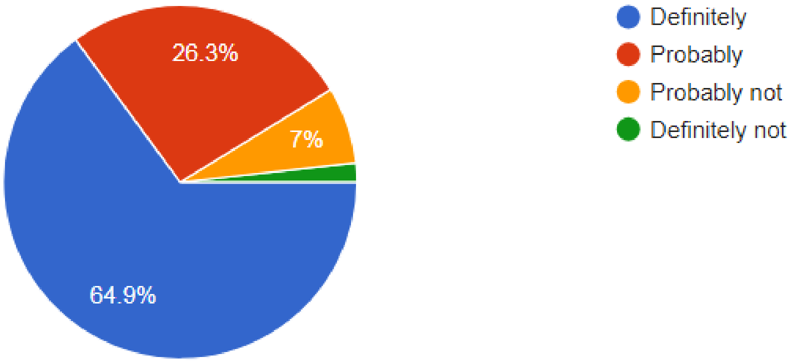

Fig.8

7. Comfort with AI Personalization and Surveillance Concerns:

Comfort with AI-driven personalization was mixed; some found it 'Somewhat comfortable,' while others were ‘Not very comfortable.’ 17.5% expressed being very comfortable with AI-driven personalized features on smartphones.

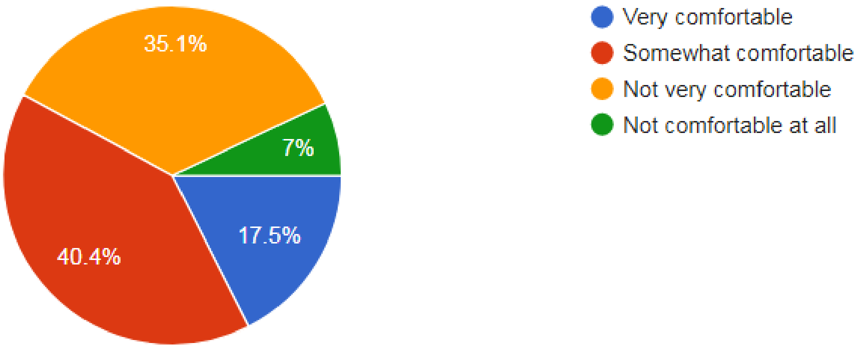

Fig.9

Concerns over potential misuse of personal information through AI-driven surveillance were prevalent, with most respondents indicating it was "Very likely."

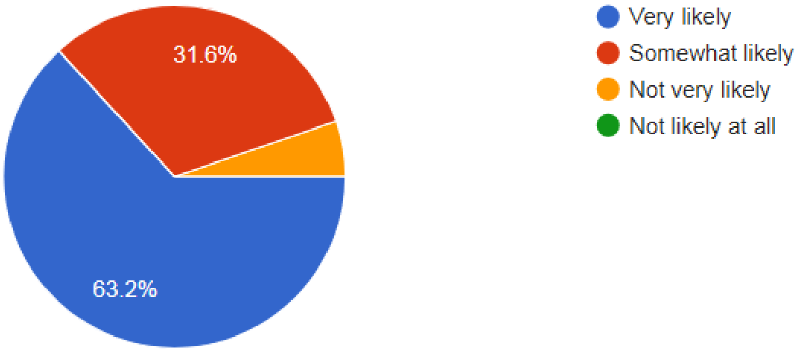

Fig.10

8. Protective Measures and Regulatory Support:

Common data protection measures included using security settings, limiting app permissions, or avoiding certain apps. There was broad support for stronger regulations on AI surveillance in smartphones to safeguard user privacy, with most respondents 'strongly supporting' these measures. Over 75.6% of respondents supported stronger laws for protection measures.

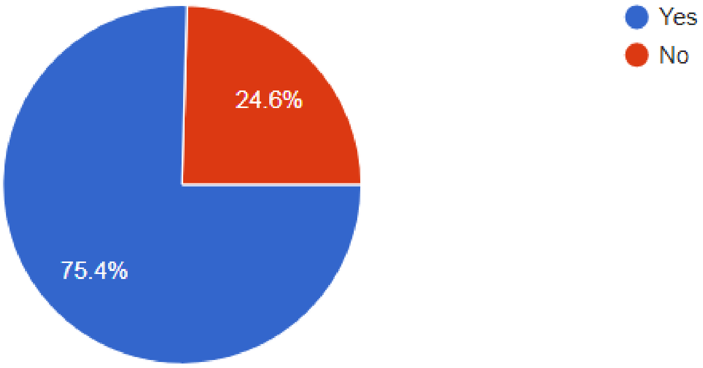

Fig.11

9. **User Experience with AI-Integrated Features**:
People experience with AI-integrated smartphone features varied; some found them "Very helpful," while others were wary, describing the technology as "Convenient but eerie."

Public Perception and Concerns on AI-Driven Features in Smartphones

The survey on the use of AI-driven features in smartphones revealed valuable insights into public awareness, privacy concerns, and user behaviors regarding AI technologies. The results indicate a nuanced understanding of AI, with respondents exhibiting a broad spectrum of familiarity with its capabilities and implications on their privacy. The findings suggest that while the use of AI is widespread, concerns about data security, surveillance, and regulatory measures remain significant issues for many users.

The survey showed a diverse demographic range, with respondents spanning a variety of age groups, professions, and educational backgrounds. The high level of familiarity with AI across these groups is noteworthy, particularly with 52.6% of respondents identifying as 'very familiar' with AI. This familiarity was not limited to those with higher education, as even individuals with lower education levels showed some awareness, with only 3.5% being unaware of AI integration in smartphones. This suggests that AI has permeated mainstream use, and public understanding of its role in modern technology is becoming more widespread, especially as educational attainment plays a role in familiarity.

When it comes to the frequency of AI feature use, the survey results indicated that while a significant portion of users engages with AI features daily, others interact with them sporadically. The most common features virtual assistants, face recognition, and personalized recommendations are used by a majority of respondents, but the intensity of their use varies. Daily usage, reported by 35.1% of participants, suggests that for many, AI has become an integrated part of their smartphone experience, with the potential to reshape daily habits and routines.

Despite this high level of usage, there is considerable concern about the role of AI in data collection. The majority of respondents were aware of how AI technologies collect data through smartphone applications, with 68.4% indicating full awareness. This awareness is linked to privacy concerns, with 61.4% of respondents expressing significant anxiety over the impact of AI on their personal privacy. This highlights a critical issue in the adoption of AI technologies: while users may be familiar with the convenience AI brings, they remain wary of the implications for their personal data.

The survey also revealed that data collection and app permissions are a source of discomfort for many. While AI features enhance user experience, respondents expressed unease with the level of data access requested by applications, which they feel compromises their privacy. The anxiety surrounding continuous monitoring of mobile activities is also evident, with 63.2% of respondents worried about their data being collected even when they are not actively using AI features. This anxiety likely contributes to a sense of powerlessness over personal information, exacerbating concerns about the extent of surveillance conducted by smartphone applications.

When respondents were made aware of excessive data collection, many expressed a willingness to stop using such apps. A significant portion (64.9%) indicated they would delete apps found to be collecting excessive data. However, a noticeable gap exists between awareness and action, as only 5% of respondents consistently read privacy policies before installing apps. This disparity suggests that while users recognize privacy risks, they may not always take the necessary steps to mitigate them beforehand.

AI-driven personalization is another area where respondents expressed mixed feelings. While 17.5% of participants reported being very comfortable with AI-driven personalized features, many others found them somewhat or not very comfortable, indicating a lack of complete trust in how personal information is used to tailor user experiences. This unease is compounded by concerns about potential misuse of personal data through AI surveillance.

To address these concerns, the survey indicated overwhelming support for stronger regulations on AI surveillance in smartphones. Over 75.6% of respondents supported the introduction of stronger laws to protect user privacy, demonstrating a widespread desire for regulatory intervention. Respondents favored protective measures such as using security settings, limiting app permissions, or avoiding certain apps, signaling that they are proactive in safeguarding their data.

While AI technologies in smartphones offer significant benefits in terms of personalization and convenience, they also raise important privacy and security concerns. The survey indicates that while users are generally familiar with AI, there is a strong desire for greater transparency, regulation, and control over personal data. Moving forward, a balance must be struck between enhancing user experiences through AI and safeguarding user privacy through stringent regulations and protective measures.

Conclusion:

The findings reiterate the profound impact of AI-driven smartphone surveillance on user privacy, autonomy, and societal norms. AI's integration with mobile technology has undoubtedly transformed how people communicate, gather information, and navigate daily tasks. However, the potential for this technology to intrude upon personal privacy and facilitate widespread surveillance has generated significant ethical, social, and psychological challenges that demand urgent attention.

The widespread use of AI in smartphones enables personalized, data-driven interactions and services, but it also amplifies data collection and privacy risks. The study highlights that users remain largely unaware of the scope of data gathered by mobile applications. Even with the rising awareness of AI's role in data collection, privacy policies, and app permissions, many users continue to overlook the degree to which their data is accessed and utilized. This sense of disempowerment over one's personal information underscores the need for transparent policies and user-friendly options to help individuals maintain control over their data.

Instances like the €290 million fine against Uber and Meta's admission of censoring COVID-19 data under government pressure serve as stark reminders of the real-world consequences of insufficient data protection measures. These examples show how companies may prioritize business interests or government pressures over user privacy and free expression. The imbalance in this relationship suggests that without adequate safeguards, companies can exploit user data with limited accountability, often at the expense of individual rights. Similarly, government surveillance measures have expanded significantly, with AI technologies enabling unprecedented levels of monitoring and control over citizens' lives.

The survey conducted in New Delhi offers insights into public awareness, concerns, and behaviors regarding smartphone AI. Findings reveal that while many users are familiar with AI features like virtual assistants and facial recognition, they remain apprehensive about privacy risks and data security. Concerns about excessive app permissions and the monitoring of user activities even when devices are not actively in use contribute to a widespread feeling of surveillance anxiety. The discomfort associated with AI-driven personalization also highlights the ambiguous relationship users have with this technology—while it offers convenience, the loss of privacy remains a significant concern.

Moreover, the survey findings underscore the tendency for self-censorship among users aware of constant surveillance. When people know that their communications and actions are being monitored, they may avoid controversial topics or disengage from activism to minimize perceived risks. This "chilling effect" poses a grave threat to free expression, as individuals may limit their speech and actions to conform to surveillance expectations. Self-censorship erodes democratic discourse and stifles the free exchange of ideas that is essential for social progress and individual freedom.

From a regulatory standpoint, the call for stricter privacy laws and data protection measures is increasingly urgent. Over 75% of survey respondents supported stronger regulations to protect user privacy, demonstrating widespread public demand for legal intervention. Governments, regulators, and tech companies must collaborate to establish clearer guidelines for data collection, transparency, and user consent. Regulatory frameworks like the European Union's General Data Protection Regulation (GDPR) have set valuable precedents by holding companies accountable for data privacy violations, but more extensive, globally coordinated efforts are needed to address the complexities of AI-driven surveillance effectively.

Beyond regulatory measures, there is a critical need for ethical standards and technological solutions to safeguard privacy in the age of AI. Developers and companies must incorporate privacy by design, ensuring that data minimization, transparency, and user control are foundational to AI systems. Privacy-enhancing technologies, such as differential privacy and federated learning, can mitigate data collection risks while still enabling personalized services. Emphasizing privacy and ethical considerations in AI development will foster a more balanced approach that respects individual rights.

The future of AI and smartphone technology must prioritize a balanced approach between innovation and privacy. If left unchecked, the normalization of AI-driven surveillance risks eroding civil liberties, autonomy, and the right to privacy. While AI has immense potential to improve everyday life, ethical and privacy considerations should be at the forefront of its implementation. Users, regulators, and tech companies all have roles to play in shaping an equitable digital landscape that upholds human dignity and freedom.

In conclusion, the study argues for the necessity of regulatory and ethical frameworks that prioritize user privacy and data security in AI-driven smartphone surveillance. Without these frameworks, the unchecked expansion of surveillance capitalism threatens to turn personal data into an exploitable commodity, with significant implications for privacy, autonomy, and democracy. By addressing these challenges proactively, society can harness the benefits of AI technology without compromising fundamental rights.

Reference

1. Ball, K., Haggerty, K. D., & Lyon, D. (2012). *Routledge Handbook of Surveillance Studies*. Routledge.
2. Bolin, G., & Jerslev, A. (2018). Surveillance through media, by media, in media. *Northern Lights*, *16*(1), 3-21.
3. Confessore, N. (2018, April 4). *Cambridge Analytica and Facebook: The scandal and the fallout so far*. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
4. Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. St. Martin's Press.
5. Fiegerman, S. (2018, April 10). *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal.* CNBC. https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html

6. Gellman, B., & Adler, C. (2019). *Dark Mirror: Edward Snowden and the American Surveillance State*. Penguin Press.
7. Khalil, H. (2024, August 26). *Uber: Dutch watchdog fines app €290m for driver data transfer*. BBC News. https://www.bbc.com/news/articles/cy76v561g48o
8. Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life*. Polity Press.
9. Lee, J. A., Liu, C. Y., & Li, W. (2012). Searching for Internet freedom in China: A case study on Google's China experience. *Cardozo Arts & Ent. LJ*, *31*, 405.
10. Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. Houghton Mifflin Harcourt.
11. Mishra, P. K. (2024, February 27). *Ai and the Legal Landscape: Embracing innovation, addressing challenges*. Live Law. https://www.livelaw.in/lawschool/articles/law-and-ai-ai-powered-tools-general-data-protection-regulation-250673
12. Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Tech. LJ*, *31*, 117.
13. Prokop, A. (2018, March 23). *The Facebook and Cambridge Analytica scandal, explained with a simple diagram.* Vox. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram
14. Purdy, S. (2015). Surveillance, Knowledge and Inequality: Understanding Power Through Foucault and Beyond. *The Hilltop Review*, *8*(1), 3.
15. **Reporters Without Borders. (2013).** *Internet surveillance: Focusing on 5 governments and 5 companies - Enemies of the Internet.* Reporters Without Borders. Retrieved from https://rsf.org/en/special-report-internet-surveillance-focusing-5-governments-and-5-companies-enemies-internet
16. Reardon, S. (2012). *Inside Iran's "halal" internet. New Scientist, 216(2886), 21.* doi:10.1016/s0262-4079(12)62625-6
17. Sipior, J. C., Ward, B. T., & Volonino, L. (2014). Privacy concerns associated with smartphone use. *Journal of Internet Commerce*, *13*(3-4), 177-193.
18. Shen, H. (2017). *Across the great (fire) wall: China and the global Internet* (Doctoral dissertation, University of Illinois at Urbana-Champaign).
19. Stewart, A., Lawrence, A., & Manvell, A. (2012). Guide to media and content regulation in Asia Pacific. *Baker & McKenzie*.
20. Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. *Columbia Law Review, 114*(3), 583-676.
21. Sweney, M. (2024, August 27). *Mark Zuckerberg says White House "pressured" facebook to censor covid-19 content*. The Guardian. https://www.theguardian.com/technology/article/2024/aug/27/mark-zuckerberg-says-white-house-pressured-facebook-to-censor-covid-19-content
22. Turkle, S. (2015). *Reclaiming Conversation: The Power of Talk in a Digital Age*. Penguin Press.
23. Watt, E. (2017). The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, *21*(7), 773-799.
24. Zuboff, S. (2020). You are now remotely controlled. *New York Times*, *24*, 2020.
25. Zuboff, S. (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs.