NEVER HAVE I EVER CHALLENGED BIOMETRIC SECURITY PRACTICES: UNVEILING GEN Z'S APPROACH AND CONCERNS TO DIGITAL IDENTITY MANAGEMENT

[1]Mr. Freddy Singaraj and [2]Dr. Rommani Sen Shitak
[1]Assistant Professor, SVKM's Mithibai College, Mumbai
[2]Head of Department - BAMMC, KPB Hinduja College, Mumbai

ABSTRACT

As the world becomes increasingly digitized, the importance of secure digital identity management practices has become more apparent. Biometric security practices are one such method that has gained popularity in recent years. With the widespread adoption of biometric technologies for authentication and identification purposes, concerns surrounding privacy have become increasingly significant. While biometric verification is often used due to the high level of security and convenience it ostensibly offers, the risk of data leaks is often overlooked. The ramifications of stolen biometric data could be drastic, as there is no way to reset biological traits like resetting a lost password.

Younger generations, such as Gen Z, are more comfortable with biometrics and are willing to use them to improve their personal security. They are increasingly driven by quality and authenticity over marketing gimmicks, and their familiarity with technology makes them the most cautious amongst all generations. However, they are also extremely private when it comes to their data, and the rise of digital connectedness during the pandemic drove an overall increase in concern about the security of personal data. As biometric authentication is expanding in authentication protocols right from banking to e-commerce, it is expected to be the future of authentication. However, current regulations around biometric data privacy are still a work in progress.

This study explores the attitudes, experiences and concerns of Gen Z individuals as they navigate the landscape of biometric digital identity and engage in a battle for privacy.

Keywords: *Biometric Authentication, Privacy, Gen Z, Digital Identity Management*

INTRODUCTION

The rapid digitisation of services across sectors such as banking, education, governance, and e- commerce has foregrounded the importance of secure digital identity management. Biometric authentication using characteristics such as fingerprints, facial recognition, or iris scans has emerged as a prominent solution due to its perceived convenience and security. However, unlike traditional passwords, biometric identifiers are permanent and irreplaceable, making their compromise particularly consequential. Generation Z, having grown up immersed in digital technologies, is often viewed as more technologically adept and adaptive. At the same time, this generation demonstrates heightened awareness of data privacy and surveillance risks, especially in the post-pandemic digital environment.

Aim: This study seeks to understand how Gen Z navigates biometric authentication systems, balancing everyday usage with concerns about privacy, control, and regulation.

RESEARCH OBJECTIVES

1. To examine Gen Z's adoption and everyday use of biometric authentication technologies.
2. To analyse Gen Z's perceptions of biometric authentication in relation to security, privacy, and trust.
3. To identify key concerns and reservations influencing Gen Z's willingness to share biometric data.
4. To explore Gen Z's expectations regarding transparency, control, and regulatory frameworks governing biometric data.

RESEARCH QUESTIONS

1. How does Gen Z adopt and integrate biometric authentication technologies into their everyday digital practices?
2. How does Gen Z perceive biometric authentication in terms of security, privacy, and trust?
3. What concerns and reservations shape Ge Z's willingness to share biometric data with institutions and organisations?
4. What expectations does Gen Z hold regarding transparency, control, and regulation of biometric

authentication systems?

METHODOLOGY

This study used a **quantitative cross-sectional survey** to examine Gen Z's perceptions and practices related to biometric authentication and digital identity management. The sample comprised **151 respondents aged 18–25**, recruited through **convenience and snowball sampling** via online platforms.

Data were collected using a **structured online questionnaire** with multiple-choice and multi- select items assessing biometric usage, perceived security, adoption likelihood, sector-wise exposure, preferred alternatives, and key concerns.

Responses were analysed using **descriptive statistics** (frequencies and percentages) to identify dominant patterns across sectors. The findings were interpreted through the lenses of the **privacy paradox** and **surveillance resignation** to contextualise high adoption alongside persistent concerns.

Participation was **voluntary and anonymous**, with informed consent obtained prior to data collection.

LITERATURE REVIEW

Digital Identity Management in a Datafied Society

Rapid digitisation has reshaped how individuals construct and manage identity. Digital identity comprises data points such as usernames, behavioural patterns, device identifiers and increasingly, biometric information (Lippold, 2017). Digital identity today is not merely a tool for access, but a mechanism through which individuals are categorised, governed and surveilled within platform- driven ecosystems (Lyon, May 2018). From a sociological perspective, online identity involves strategic self-presentation, where individuals continuously negotiate visibility and privacy across digital spaces (Goffman, 1956). As digital platforms require constant authentication, identity has become more fixed, traceable and data-driven. This paves the way for biometric technologies, which offer convenience but raise questions about autonomy, consent and control.

Biometric Authentication Technologies: Convenience Versus Risk

Biometric authentication uses unique biological or behavioural traits such as fingerprints, facial features, iris patterns or voice recognition to verify identity (Jain, Ross, & Prabhakar, Jan 2024). Promoted as more secure and efficient than passwords, biometrics are now widely used across banking, smartphones, e-commerce and government services, making them central to digital identity management.

Despite their efficiency, biometric identifiers differ fundamentally from traditional authentication mechanisms. Unlike passwords, biometric traits are permanent and cannot be changed once compromised, rendering breaches particularly consequential (Woodward, 1997). (Cavoukian, 2011) Ann Cavoukian further cautions against function creep, wherein biometric data collected for authentication may later be repurposed for surveillance, profiling or commercial exploitation.

Privacy, Surveillance and Biometric Data

Privacy remains a central concern in discussions of biometric technologies. Classical definitions frame privacy as control over personal information (Westin, 1967), while contemporary approaches emphasise contextual integrity and appropriate data flows (Nissenbaum, 2009). Biometric data is widely recognised as highly sensitive due to its direct link to bodily identity, requiring heightened ethical and regulatory safeguards (Solove, 2006).

Surveillance scholars argue that biometric technologies normalise monitoring by embedding identification mechanisms into everyday digital practices (Lyon, May 2018). (Zuboff, 2019) explains biometric data as part of *surveillance capitalism*, where personal information is constantly collected and monetised. This process reduces users' control over their data and encourages passive acceptance, making people less likely to question or resist biometric security practices.

Digital Identity practices, Privacy paradox and Non-Challenging Behaviour of Gen Z

While Prensky frames Digital Natives as technologically fluent users, his study predates Gen Z's concerns around biometric surveillance, privacy, and digital identity (Prensky, 2001). Research suggests that Gen Z values efficiency, authenticity and personalisation, making them more receptive to innovations such as biometric authentication (Seemiller & Grace, 2016). Despite this openness, studies indicate that Gen Z demonstrates heightened awareness of data privacy risks, including concerns about surveillance and data misuse (Auxier, Rainie, Anderson, & Andrew Perrin, 2019). This coexistence of technological comfort and privacy concern positions Gen Z as a critical group for examining how biometric security practices are perceived and negotiated. Privacy research highlights the "privacy paradox," where users express concern about data privacy yet continue using data-intensive technologies, driven by limited alternatives, surveillance resignation, and power imbalances between users and platforms (Barth & Jong, 2017) (Boyd, 2014) (Zuboff, 2019).

Regulatory Frameworks

The governance of biometric data varies significantly across regions. Frameworks such as the European Union's General Data Protection Regulation (GDPR) classify biometric data as sensitive personal data and mandate strict conditions for its processing (General Data Protection Regulation (GDPR), 2018). In contrast, many countries, including India, continue to develop and refine their data protection laws, resulting in regulatory uncertainty around consent, data storage and accountability (Bennett & Raab, 2006)

Research Gap

While studies on biometric authentication have focused on technical and policy dimensions, Gen Z's lived experiences and privacy negotiations particularly in urban India remain underexplored. This study addresses this gap by exploring how Gen Z individuals perceive, experience and contest biometric security practices, thereby contributing to a more nuanced understanding of youth, privacy and digital identity in an increasingly biometric-driven world.

FINDINGS

Gen Z's Adoption, Integration and Concerns of Biometric Authentication into Daily Life

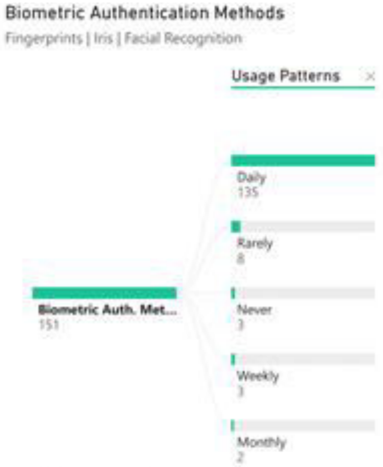


Fig 1.1

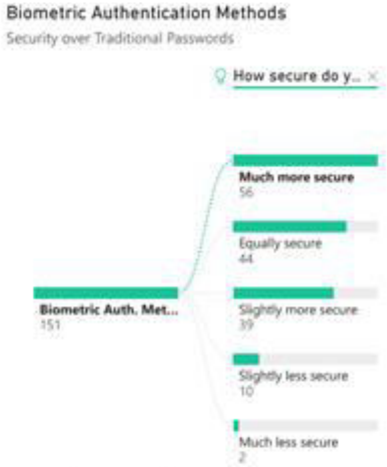


Fig 1.2

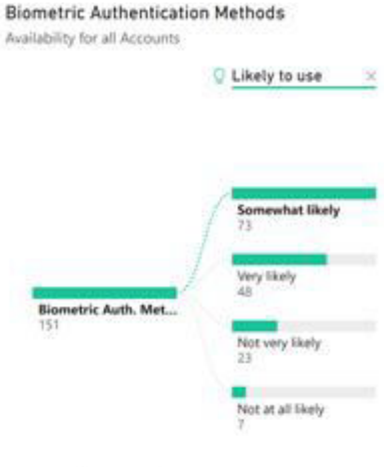


Fig 1.3

(Fig 1.1) The participants were asked about the frequency with which they use biometric authentication methods like fingerprint, iris scan, facial recognition etc. to access their devices or accounts. Out of 151 respondents, **135 (89%)** reported using biometric authentication **daily**, indicating its deep integration into everyday digital practices. Only **8 participants (5%)** used biometrics rarely, while **3 (2%)** reported never using them. Occasional usage was minimal, with **3 respondents (2%)** using biometrics weekly and **2 (1%)** monthly. This suggests a strong **normalisation and habitual reliance** on biometric security systems among Gen Z. Despite broader concerns around privacy and surveillance, daily use appears driven by convenience and system dependence. This pattern reflects a pragmatic acceptance of biometric technologies rather than active resistance.

(Fig 1.2) The participants were asked to compare the security of biometric authentication methods with traditional passwords. Out of 151 respondents, **56 participants (37%)** perceived biometric authentication as **much more secure** than traditional passwords, indicating strong confidence in biometric systems. An additional **39 respondents (26%)** felt biometrics were **slightly more secure**, reinforcing an overall positive security perception. However, **44 participants (29%)** viewed biometric methods as **equally secure**, suggesting a more cautious or balanced assessment. A small minority expressed scepticism, with **10 respondents (7%)** rating biometrics as **slightly less secure** and **2 respondents (1%)** as **much less secure**. Overall, the data shows that Gen Z largely perceives biometric authentication as at least as secure if not more secure than passwords.

(Fig 1.3) The participants were asked to indicate their likelihood of using biometric authentication methods if they were available for all their accounts. Out of 151 respondents, **73 participants (48%)** indicated they were **somewhat likely** to use biometric authentication if it were available for all accounts, while **48 respondents (32%)** reported being **very likely** to adopt it. In contrast, **23 participants (15%)** were **not very likely**, and **7 respondents (5%)** were **not at all likely** to use biometrics across all accounts. Overall, **80%** of the respondents expressed at least some willingness to adopt biometric authentication universally. This suggests a

ISSN 2394 - 7780

generally positive orientation toward biometrics, tempered by cautious consideration rather than unconditional acceptance.

Genz's Authentication Alternatives, Encounters and Primary Concerns with Biometric Authentication Methods

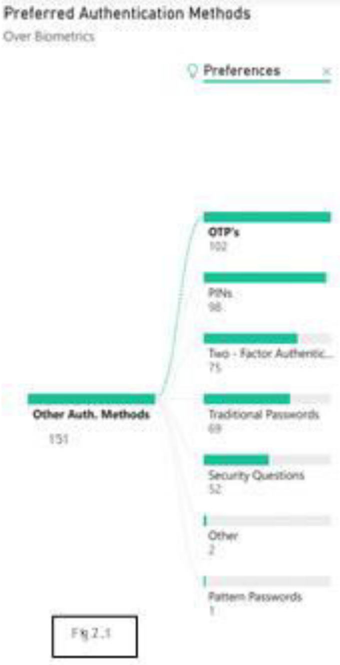


Fig 2.1

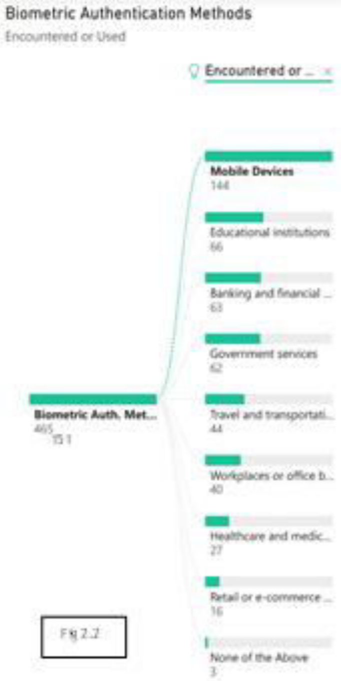


Fig 2.2

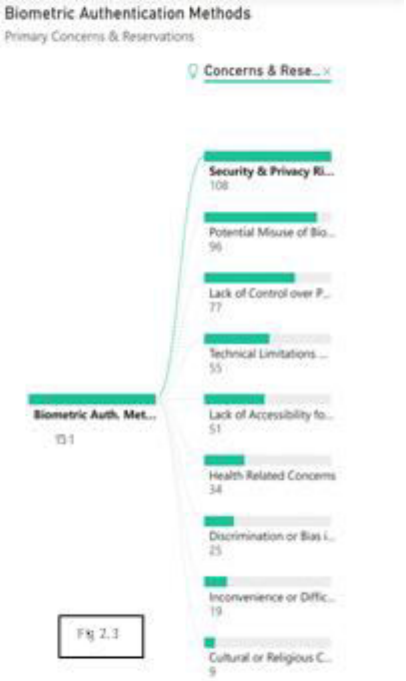


Fig 2.3

(Fig 2.1) The participants were asked to select their preferred authentication methods over biometrics from a list of options. When asked to choose preferred authentication methods over biometrics, respondents showed a clear inclination toward **knowledge- and multi-step-based security options**. **OTPs were the most preferred (102 respondents, 68%)**, closely followed by **PINs (98, 65%)**, indicating trust in controllable, revocable credentials. **Two-factor authentication was selected by 75 respondents (50%)**, reinforcing the value placed on layered security. Notably, **69 respondents (46%)** still preferred **traditional passwords**, while **52 (34%)** chose **security questions**. Overall, the findings suggest that despite high biometric usage, Gen Z retains a strong preference for authentication methods that offer **greater perceived control and recoverability**, reflecting underlying concerns about permanence and misuse of biometric data.

(Fig 2.2) Participants were asked to select the sectors in which they have encountered or used biometric authentication methods. The data shows that biometric authentication is most commonly encountered in **mobile devices**, with **144 respondents (95%)** reporting usage, underscoring its role as an everyday access mechanism. Beyond personal devices, biometrics were frequently experienced in **educational institutions (66 respondents, 44%)**, **banking and financial services (63, 42%)**, and **government services (62, 41%)**, indicating institutional normalisation of biometric systems. Moderate exposure was reported in **travel and transportation (44, 29%)** and **workplaces or office buildings (40, 26%)**. Fewer respondents encountered biometrics in **healthcare settings (27, 18%)** and **retail or e-commerce contexts (16, 11%)**. Overall, the findings suggest that Gen Z's engagement with biometrics spans both personal and institutional domains, reinforcing their routine acceptance while also expanding the scope of biometric data collection across everyday life.

(Fig 2.3) Participants were asked to select their primary concerns or reservations about biometric authentication methods. The findings reveal that **security and privacy risks** are the most prominent concern, selected by **108 respondents (72%)**, followed closely by **potential misuse of biometric data** (**96 respondents, 64%**).

A significant proportion also expressed anxiety over **lack of control over personal information** (**77 respondents, 51%**), highlighting issues of data ownership and consent. **Technical limitations and reliability issues** were noted by **55 respondents (36%)**, while **lack of accessibility for individuals with disabilities** concerned **51 respondents (34%)**. Fewer participants identified **health-related concerns** (**34 respondents, 23%**) and **discrimination or bias in biometric systems** (**25 respondents, 17%**). Overall, the pattern suggests that Gen Z's reservations are driven more by **systemic privacy, control, and governance issues** than by everyday usability or cultural concerns.

Gen Z's Sector-specific Insights for Biometric Authentication Adoption, Caution and Avoidance

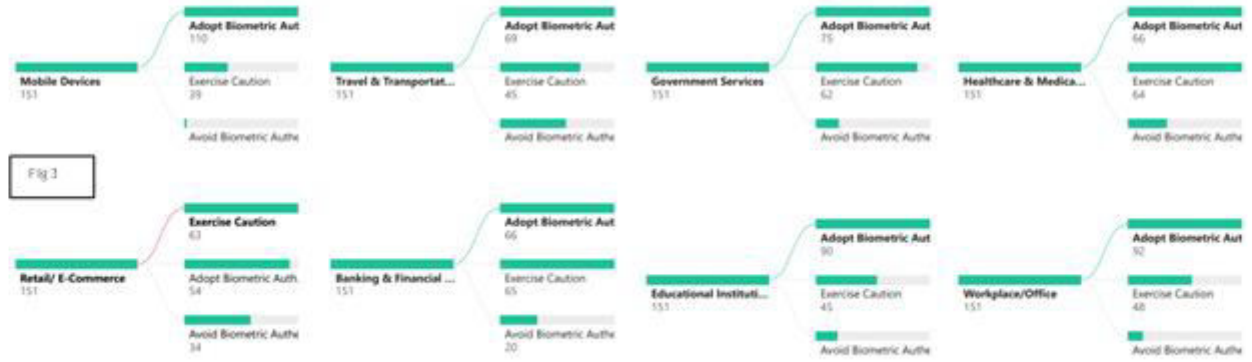


Fig 3

The question asked participants to indicate which sectors should prioritize the adoption of biometric authentication methods, and which sectors should exercise caution or avoid using them altogether. The data indicates strong support for adopting biometric authentication in **mobile devices (110 respondents, 73%)**, **workplaces/offices (92, 61%)**, and **educational institutions (90, 60%)**, suggesting comfort with biometrics in routine and regulated environments. **Government services** saw **75 respondents (50%)** favouring adoption, closely followed by **62 (41%)** urging caution, reflecting ambivalence around state-managed data. In **banking and financial services**, adoption (**66, 44%**) and caution (**65, 43%**) were almost evenly split, highlighting heightened sensitivity to financial risk. **Healthcare** showed a similar divide, with **66 respondents (44%)** supporting adoption and **64 (42%)** recommending caution due to data sensitivity. **Travel and transportation** leaned towards adoption (**69, 46%**) but retained notable caution (**45, 30%**). **Retail and e-commerce** emerged as the most contested sector, with **63 respondents (42%)** favouring caution over adoption (**54, 36%**), indicating greater resistance to biometric use in commercial contexts. *While there is widespread support for biometric adoption in mobile devices, educational institutions, workplaces, and certain sectors like healthcare and government services, there are concerns and reservations in sectors such as banking and financial services, travel and transportation, and retail or e-commerce.*

Gen Z's Attitudes towards Provisions of Biometric Data Collection, Storage and Use by Companies and Educational Institutions

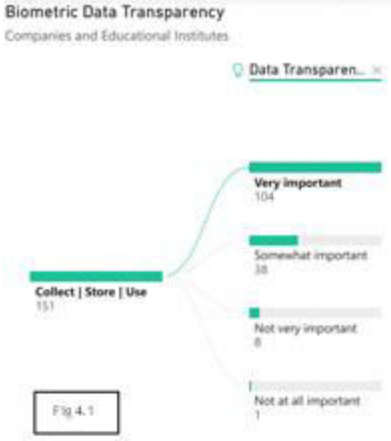

Biometric Data Transparency
Companies and Educational Institutes

Fig 4.1

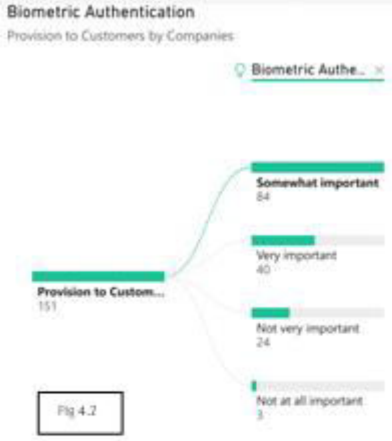

Biometric Authentication
Provision to Customers by Companies

Fig 4.2

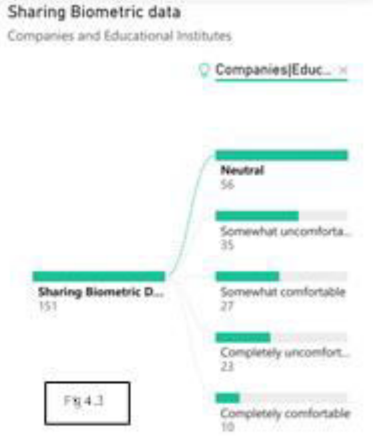

Sharing Biometric data
Companies and Educational Institutes

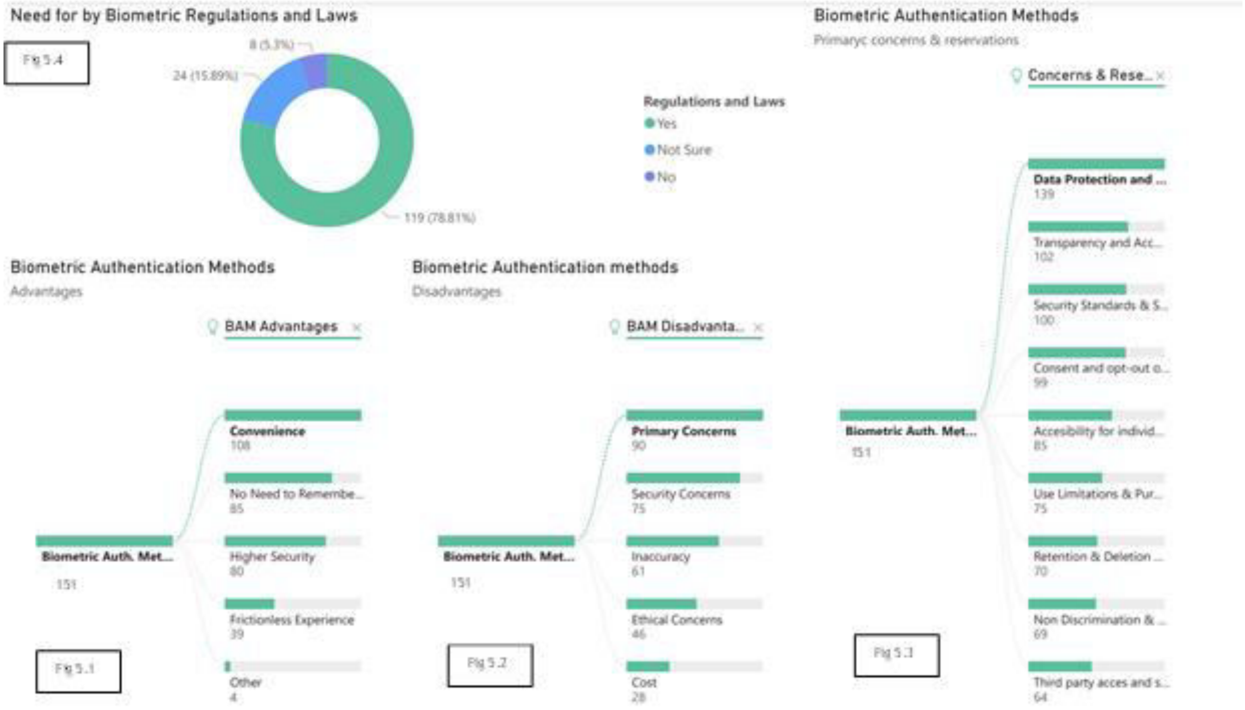
Fig 4.3

The findings show an overwhelming emphasis on **transparency in biometric data practices** among respondents. A clear majority, **104 participants (69%)**, rated transparency in the collection, storage and use of biometric data as **very important**, while an additional **38 respondents (25%)** considered it **somewhat important**. Only a small minority viewed transparency as less critical, with **8 respondents (5%)** rating it **not very important** and just **1 respondent (0.7%)** indicating it was **not at all important**. Overall, **94%** of participants expressed that transparency matters to them to some degree. This underscores Gen Z's strong expectation for **institutional accountability, clarity and informed consent** in biometric data governance, even as they continue to engage with biometric systems in everyday contexts.

(Fig 4.2) Participants were asked to rate the importance of companies providing biometric authentication options for their customers. The data suggests a generally positive but measured attitude toward companies offering biometric authentication options. **84 respondents (56%)** rated the provision of biometric authentication as **somewhat important**, while **40 respondents (26%)** considered it **very important**. In contrast, **24 participants (16%)** felt it was **not very important**, and only **3 respondents (2%)** viewed it as **not at all important**. Overall, **82%** of respondents assigned at least some importance to companies providing biometric options. This indicates that while Gen Z values the availability of biometric authentication, they may prefer it as an **optional or supplementary feature** rather than a mandatory requirement.

(Fig 4.3) Participants were asked to express their feelings about sharing their biometric data with private companies or educational organizations. The data reveals a **mixed and cautious stance** toward sharing biometric data with private companies and educational institutions. The largest group of respondents, **56 participants (37%)**, expressed a **neutral** position, indicating ambivalence or conditional acceptance. A notable proportion reported discomfort, with **35 respondents (23%)** feeling **somewhat uncomfortable** and **23 respondents (15%)** feeling **completely uncomfortable**, together accounting for **38%** of the sample. In contrast, fewer participants expressed comfort, with **27 respondents (18%)** being **somewhat comfortable** and only **10 respondents (7%) completely comfortable**. Overall, the findings suggest that while Gen Z may comply with biometric data sharing, this acceptance is often accompanied by hesitation and emotional unease rather than confidence or trust.

Shaping the Legal Framework: Gen Z's Perspective and Reservations



(Fig 5.1) Participants were asked to identify the advantages of using biometric authentication methods over traditional passwords. The findings show that **convenience** is the most prominent advantage of biometric authentication, selected by **108 respondents (72%)**, underscoring ease and speed of access as key drivers. This is followed by **not needing to remember passwords**, cited by **85 respondents (56%)**, highlighting relief from cognitive burden. **Higher security** was identified by **80 respondents (53%)**, indicating that over half associate biometrics with enhanced protection. A smaller proportion, **39 respondents (26%)**, valued the **frictionless user experience**, suggesting usability benefits are acknowledged but secondary.

Very few respondents (**4, 3%**) cited other advantages. Overall, the data suggests that Gen Z's preference for biometrics is shaped more by **practical convenience and usability** than by security considerations alone.

(Fig 5.2) Participants were asked to identify the disadvantages of using biometric authentication methods. The data shows that concerns around biometric authentication are led by broad **primary concerns**, selected by **90 respondents (60%)**, indicating overarching unease about the technology. **Security concerns** were cited by **75 respondents (50%)**, reflecting fears related to data breaches and misuse. **Inaccuracy** was highlighted by **61 respondents (40%)**, suggesting doubts about reliability and error rates. **Ethical concerns**, including issues of consent and surveillance, were noted by **46 respondents (30%)**. **Cost** emerged as the least significant disadvantage, selected by **28 respondents (19%)**. Overall, the findings indicate that Gen Z's reservations are centred more on **trust, reliability, and ethical implications** than on financial considerations.

(Fig 5.3) Participants were asked to identify the aspects they believed laws and regulations over biometric authentication methods should cover. Out of 151 participants, **data protection and privacy** emerged as the most critical regulatory aspect, selected by **139 respondents (92.05%)**. This was followed by **transparency and accountability** (**102 respondents; 67.55%**) and **security standards and safeguards** (**100 respondents; 66.23%**), indicating strong expectations around institutional responsibility. **Consent and opt-out options** were prioritised by **99 respondents (65.56%)**, underscoring the importance of user control. **Accessibility for individuals with disabilities** was identified by **85 respondents (56.29%)**, reflecting inclusivity concerns. Regulatory focus on **use limitations and purpose restrictions** (**75 respondents; 49.67%**) and **retention and deletion of biometric data** (**70 respondents; 46.36%**) received moderate support. Finally, **non-discrimination and fairness** (**69 respondents; 45.70%**) and **third-party access and data sharing** (**64 respondents; 42.38%**) were comparatively lower, yet still notable considerations.

(Fig 5.4) The participants were asked whether they believed there should be specific regulations or laws governing the use of biometric authentication methods. The findings indicate a **strong consensus in favour of regulatory oversight** for biometric authentication methods. A clear majority of participants, **119 respondents (78.81%)**, believe that **specific laws and regulations are necessary**, reflecting widespread concern about the governance of biometric technologies. Meanwhile, **24 participants (15.89%)** reported being **uncertain**, suggesting partial awareness or unresolved trust in existing safeguards. Only a small minority, **8 respondents (5.30%)**, felt that such regulations are **not required**. Overall, the data highlights **high public support for formal regulatory frameworks**, with minimal outright resistance, underscoring the perceived risks and sensitivities associated with biometric data use.

INTERPRETATION OF FINDINGS IN RELATION TO THE RESEARCH QUESTIONS

RQ1: How does Gen Z adopt and integrate biometric authentication into everyday digital practices?

The findings show that biometric authentication is deeply embedded in Gen Z's daily digital routines, indicating strong normalisation. However, this integration reflects pragmatic compliance rather than active choice. As Cheney-Lippold (2017) argues, digital identity has become infrastructural and datafied, limiting users' ability to opt out. Biometric systems therefore function as default access mechanisms rather than voluntarily adopted security practices.

RQ2: How does Gen Z perceive biometric authentication in terms of security, privacy, and trust?

Gen Z generally perceives biometrics as equal to or more secure than passwords, yet this trust is conditional and context-dependent. Drawing on Nissenbaum's (2010) concept of contextual integrity, acceptance hinges on how biometric data is governed, including transparency, purpose limitation, and accountability, rather than on technical security alone.

RQ3: What concerns shape Gen Z's willingness to share biometric data?

Despite high adoption, respondents express persistent concerns around privacy, misuse, and loss of control. Preferences for revocable alternatives such as OTPs and two-factor authentication highlight a desire for agency. This contradiction reflects the privacy paradox (Barth & de Jong, 2017) and aligns with Zuboff's (2019) argument that surveillance capitalism fosters resignation rather than resistance.

RQ4: What expectations does Gen Z hold regarding transparency, control, and regulation?

Strong support for regulation, consent, and transparency underscores ethical unease with biometric expansion. Sector-specific caution, particularly toward commercial and state contexts, supports Lyon's (2018) view that surveillance becomes most contested when identification systems extend beyond personal utility into institutional monitoring.

CONCLUSION

This study set out to examine how Generation Z navigates biometric authentication systems amid growing concerns around privacy, control, and digital identity governance. The findings reveal that biometric technologies are deeply embedded in Gen Z's everyday digital practices, particularly through smartphones and institutional platforms. However, this widespread adoption does not signify unquestioned trust. Instead, Gen Z's engagement with biometrics reflects a form of negotiated acceptance shaped by convenience, limited alternatives, and structural dependence on platform-driven authentication systems.

While respondents largely perceive biometric authentication as secure and efficient, their trust remains conditional and context-dependent. Persistent concerns around data misuse, loss of control, and permanence of biometric identifiers indicate that security is understood not merely as a technical attribute, but as an outcome of ethical governance, transparency, and accountability. The preference for revocable authentication alternatives further underscores Gen Z's desire for agency in managing digital identity, revealing a clear manifestation of the privacy paradox, where concern coexists with continued compliance.

Importantly, the study highlights Gen Z's strong expectations for regulatory oversight, consent mechanisms, and transparency in biometric data practices. Sector-specific variations in acceptance demonstrate that trust is shaped by institutional power and perceived risk, with heightened caution toward commercial and state-managed contexts.

By foregrounding Gen Z's lived experiences within an urban Indian context, this research contributes to ongoing debates on biometric surveillance, digital identity, and youth privacy. It underscores the urgent need for robust regulatory frameworks that balance technological innovation with user rights, ensuring that biometric systems operate within ethically grounded and democratically accountable structures.

BIBLIOGRAPHY

Lippold, J. C. (2017). We Are Data: Algorithms and the Making of Our Digital Selves. New York University press.

Lyon, D. (May 2018). In D. Lyon, *The Culture of Surveillance: Watching as a Way of Life.*

(1959). In E. Goffman, *The Presentation of Self in Everyday Life.* Scotland: Doubleday.

Goffman, E. (1956). The Presentation of Self in Everyday Life. In E. Goffman. Scotland: Doubleday. Jain, A. K., Ross, A., & Prabhakar, S. (Jan 2024). An introduction to biometric recognition. *IEEE*

Transactions on Circuits and Systems for Video Technology, 4-20.

Woodward, J. (1997). Biometrics: privacy's foe or privacy's friend? *Proceedings of the IEEE*, 1480-1492. Cavoukian, A. (2011). Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and

Trust in the Information Era.

Westin, A. (1967). *Privacy and freedom.* New York: Atheneum.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford Law & Politics.

Solove, D. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review,*, 477–560. Zuboff, S. (2019). *The age of surveillance capitalism.* PublicAffairs.

Prensky, M. (2001). Digital natives, digital immigrants. . *On the Horizon*, 1-6. Seemiller, C., & Grace, M. (2016). *Generation Z Goes to College.* Jossey-Bass.

Auxier, B., Rainie, L., Anderson, M., & Andrew Perrin, M. K. (2019). *Americans and privacy: Concerned, confused and feeling lack of control over their personal information.* Pew Research centre.

Barth, S., & Jong, M. D. (2017). The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior. *Telematics and Informatics 34(7).*

Boyd, D. (2014). *It's Complicated: The Social Lives of Networked Teens.* Yale University Press. (2018). *General Data Protection Regulation (GDPR).* Official Journal of the European Union. Bennett, C. J., & Raab, C. D. (2006). *The Governance of Privacy: Policy Instruments in Global*

Perspective. Routledge.