Online Anonymity vs. Online Accountability

Gabrielle Olds
Computer Science
Hampton University
Hampton, Virginia
gabrielle.olds@my.hamptonu.edu

Abstract

The main problem with the conflict between online anonymity and accountability is that, although anonymity promotes privacy and free speech, it also makes harmful behaviors like trolling and scams possible. In order to understand how mandatory identification policies, like requiring government IDs or facial scans for site access, affect this balance, this study will review previous research. Privacy and security risks will be a major focus because private businesses collect extremely sensitive data, increasing the risk of data breaches, long-term identity theft, and user tracking. In order to make fair policy decisions, a survey will also be carried out to find out how the public feels about these intrusive verification techniques.

I. Introduction

Today, the internet plays a major role in modern life, influencing how people communicate and share information, whether or not they do so anonymously. This brings about the issue of how to strike a balance between accountability and online anonymity. Anonymity can be beneficial because it protects privacy and promotes free speech, particularly when doing so could put one in danger politically or socially. However, anonymity also makes it possible for negative actions like harassment, false information, and fraud, which brings light to questions about the security and reliability of online environments.

Reducing anonymity through more intrusive identification requirements, such as government-issued IDs or biometric scans, is a proposed solution. These are reflected in laws like the UK's Online Safety Act of 2023, which puts pressure on platforms to strengthen verification procedures in order to protect users, especially children. It's arguable that holding users accountable can discourage harmful behavior; however, privacy, identity theft, and long-term data security risks should also be considered. These concerns highlight the need for a more thorough examination of the possible advantages and disadvantages of decreasing anonymity. This research will address three main questions: Does eliminating anonymity decrease harmful online behavior? Are the security risks of collecting sensitive IDs justified by the benefits? And how do users weigh digital freedom against the need for safety? By addressing these questions, a better understanding of how society can responsibly navigate the tension between anonymity and accountability in the digital world could be met.

II. Methodology

This study employs a mixed-methods approach comprising a literature review and a public opinion survey. Together, these methods provide both theoretical insight and empirical data on how users perceive online identity verification and the loss of anonymity.

The literature review synthesizes scholarly research, policy analyses, and real-world case studies related to online anonymity, digital identity verification, privacy risks, and regulatory frameworks. Sources include academic journal articles, government policy analyses, cybersecurity studies, and investigative news reporting. The review examines themes such as anonymity-related online aggression, risks associated with biometric and ID-based verification systems, the regulatory pressures introduced by the Online Safety Act and the Digital Services Act, and documented incidents in which verification data were compromised. These themes guide the interpretation of the survey findings and establish the theoretical foundation for the study.

The quantitative survey was developed using Google Forms and distributed across LinkedIn, Instagram, and Facebook to gather a broad range of public opinions. The survey included multiple-choice, scaled, and open-ended questions that asked participants about their comfort levels with providing government-issued identification and biometric information, their perceptions of the risks associated with data collection and identity theft, and their views on whether verification increases online safety or simply threatens personal privacy. Respondents were also asked about their social media usage, including how active they are on their accounts and the purposes for which they use these platforms. The survey remained open for several days, collecting responses anonymously. No personally identifiable information was requested, and all responses were analyzed in aggregate to ensure participant privacy.

III. Literature Review

Research on digital identity consistently demonstrates that online anonymity and accountability exist in a delicate and often contradictory relationship, shaping both user safety and user privacy. Scholars widely acknowledge that anonymity can create opportunities for harmful online behavior. Still, they emphasize that identity verification systems pose significant risks—including data breaches, surveillance, and expanded corporate power over user information. This body of literature suggests that the debate is not simply about choosing anonymity or accountability, but about managing the complex trade-offs between them.

A strong theme in existing research is the link between anonymity and increased online aggression. Moore et al. found that cyberbullies and individuals who post hostile or inflammatory content often rely on anonymous or pseudonymous identities to avoid social, legal, or reputational consequences. Their findings align with other behavioral research demonstrating the “online disinhibition effect,” where anonymity lowers social cues and increases impulsivity, leading to harassment, hate speech, and other forms of misconduct. Similar patterns emerge in studies on digital transactions. Sree and Damodaram argue that the absence of identity

verification in online exchanges can contribute to fraud, impersonation, and various forms of financial exploitation. Together, these studies indicate that certain forms of anonymity soften accountability structures and create environments where harmful or unlawful behavior can flourish.

However, the literature consistently warns that identity verification is not a straightforward solution. Malik's work on biometric authentication highlights that systems relying on facial recognition, fingerprints, iris scans, or government-issued IDs introduce substantial risks. Biometric data, unlike passwords, cannot be replaced if compromised, creating permanent vulnerabilities for individuals whose information is stolen. Scholars also point out that verification systems often rely on centralized databases that store millions of sensitive records, making them highly attractive targets for cybercriminals. This concentration of data expands the impact of individual breaches and raises questions about whether platforms should be trusted with such sensitive information in the first place.

Real-world incidents vividly illustrate these dangers. Booth's reporting on the Discord age-verification breach shows how even systems intended to enhance safety can expose users to new threats. The leak of tens of thousands of government ID photos underscores the fragility of third-party verification vendors and the potential consequences of inadequate data protection. These events support claims made in the scholarly literature that identity verification may unintentionally create a new layer of risk. One that affects users long after the immediate harm of harassment or misinformation has subsided.

Regulatory pressures add another dimension to the complexity of online identity. Law's analysis of the UK's Online Safety Act (OSA) and the EU's Digital Services Act (DSA) shows how governments are increasingly requiring platforms to impose stricter identity checks, conduct risk assessments, and monitor user behavior. While these policies aim to reduce harmful content and protect vulnerable users, particularly minors, they also shift significant surveillance responsibilities onto private companies. Scholars argue that such legislative frameworks could normalize invasive data collection and gradually erode the right to anonymity online. Additionally, platforms may face incentives to "over-comply," collecting more data than necessary in order to avoid legal penalties, further increasing privacy and security risks for users.

Across this literature, a major tension emerges: anonymity is frequently portrayed as both a shield and a weapon. It can protect vulnerable groups, including activists, whistleblowers, LGBTQ+ individuals, and political dissidents who rely on anonymity to speak safely. At the same time, anonymity can cause harassment, extremist recruitment, and the spread of harmful misinformation. On the other hand, identity verification may discourage harmful behavior by strengthening accountability, but may also expose users to surveillance, identity theft, and long-term data insecurity. This underscores the need to treat online anonymity not as a binary attribute but as a spectrum with varying degrees of risk and benefit depending on context.

Because of these challenges, a growing number of researchers advocate for privacy-preserving identity solutions. Technologies such as zero-knowledge proofs, decentralized digital credentials, and “tokenized” age verification allow platforms to confirm user attributes (like age) without collecting or storing identifying information. These innovations reflect a larger shift in the literature toward finding hybrid models that preserve anonymity where possible while enabling accountability where necessary.

Overall, the literature shows clearly that neither unrestricted anonymity nor strict identity verification can fully resolve the challenges of digital safety. Instead, researchers increasingly emphasize the need for nuanced, balanced approaches that consider technical feasibility, human behavior, privacy rights, and the social consequences of data misuse. This ongoing tension between safety and privacy forms the foundation of the present study, which examines how the public perceives these trade-offs and how willing users are to accept security risks in exchange for accountability,or vice versa.

IV. Results and Analysis

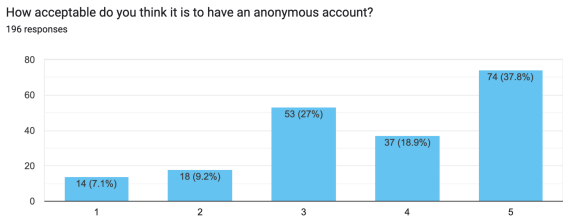
This section presents the findings of the online public survey, which was designed to quantify user perspectives on the core tension between online anonymity, accountability, and security risks. The data is analyzed to address the three primary research questions.

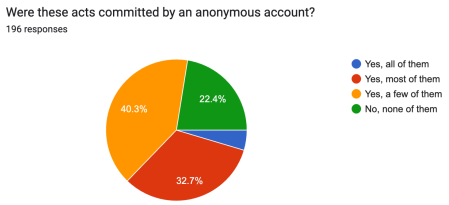
1. The Link Between Anonymity and Harm

The first main point is looking at the efficacy of eliminating anonymity as a way to decrease harmful behavior online.

Damage and Attribution of the Source

According to the survey, there is a high level of exposure to online misconduct: 87.3% of all respondents said they have either directly experienced or witnessed harmful behavior (hate speech, scams, harassment, etc.). The data revealed a strong public correlation between anonymity and malicious acts when asked to identify the cause of this harm. 87.8% of those who reported being harmed or witnessing harm said that an anonymous account was responsible.





The underlying premise of accountability laws, that a large percentage of online misconduct is the result of non-identifiable users, is strongly supported by this finding. The correlation is especially pronounced among those most frequently exposed to harm: 97.3% of respondents who reported experiencing "Yes, many" instances of harmful behavior attributed

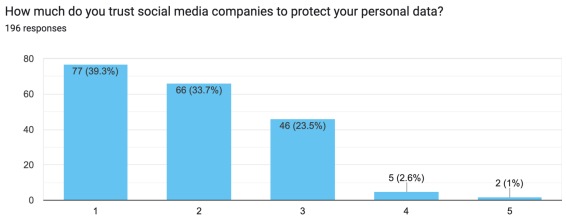
those acts, at least partially, to an anonymous account. Furthermore, 79.7% of all respondents believe that being anonymous gives people "courage" to post things they normally wouldn't, suggesting a strong public recognition that anonymity leads to harmful happenings. This combined evidence suggests that raising verification standards would potentially improve user safety by directly addressing the perceived cause of most online harm. However, this belief is not unanimous, as only 43.8% of respondents who experienced anonymous harm agree that verification would fully reduce misconduct.

2. User Trust, Security Risks, and Verification Compliance

The second point looked into whether the security risks in collecting sensitive identification data are justified by the possible benefits of increased accountability.

Decrease in Trust and Verification Willingness

User trust in the data protection capabilities of social media companies was low. On a 5-point scale, with 1 being “Not at all trustworthy” and 5 being “Completely trustworthy”, the average score was 2.8, indicating general skepticism. Furthermore, 73.1% of respondents were shown as having "Low Trust" (scoring 1 or 2). This lack of faith is compounded by severe user concern, with 36.5% of all respondents reporting they are "Extremely concerned" (score 5) about data breaches or identity theft.



The willingness to use intrusive verification techniques showed some conflict despite this trust gap. Forty percent of those in the Low Trust category still indicated that they were "willing" or "maybe willing" to provide a government-issued ID or a facial scan to confirm their age or identity.

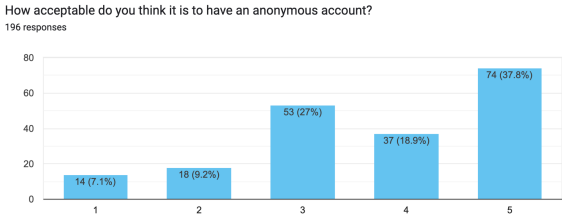
This data shows an interesting conflict in that a segment of the population is willing to overlook well-known security flaws, such as low trust and the possibility of a data breach, in favor of the benefits of online access or enhanced platform security. However, the data highlights that for the wider user base, the risk of ID collection is a serious deterrent: the most concerned users (75.0% of the highly concerned group [score 5] chose the lowest comfort scores of 1 or 2), indicating a strong rejection of the security trade-off. Even among the least concerned, 75.0 chose the lowest comfort score, highlighting a reluctance that mandatory verification must overcome. Nonetheless, the results show that public trust is important for a successful and moral implementation of mandatory verification policies, since most members of the Low Trust group are still reluctant to give out sensitive information.

3. The Practical Benefits of Anonymity

The final question seeks to understand how users weigh online freedom (anonymity) against the need for safety, and recognizes the use of anonymous accounts.

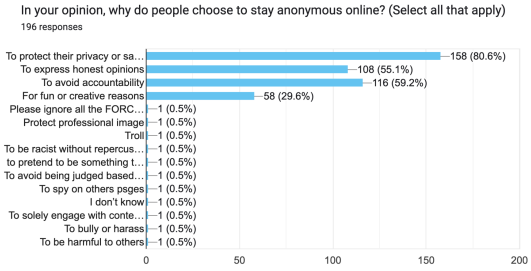
Acceptability and Motivation

The overall acceptability of anonymous accounts was high, with an average score of 4.1 out of 5. 38.1% of respondents rated anonymity as "Very Acceptable" (score 5), showing that users view anonymity as a fundamental and legitimate aspect of online interaction. However, only 31.0% of respondents believe that the benefits of online anonymity outweigh its potential harms, indicating that the public values the *option* of anonymity while remaining skeptical of its net positive societal effects.



When participants were asked to identify the main reason people choose to use anonymous accounts, the responses overall focused on protective and expressive perspectives:

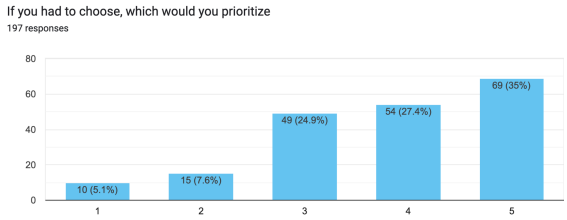
1. To protect their privacy or safety (80%)
2. To express honest opinions (55%)
3. To avoid accountability (59%)



According to the data, the public views anonymity mainly as a shield or an essential tool for unrestricted free speech and privacy protection. Fewer than half of users who cite protective reasons draw attention to its role in evading responsibility and committing misconduct. The majority of users who use anonymity for legitimate, protective purposes must not be negatively impacted by any policy that attempts to reduce it. According to the survey's findings, policies must be specifically designed to address the 30% concern without sacrificing the 70% necessity.

The Cost of Safety

This necessity for anonymity creates a policy dilemma, as shown in the section concerning the trade-off between freedom and safety. When asked to prioritize, the public leans toward safety, but the belief that mandatory verification restricts speech is widespread. Even among the group that most highly prioritizes Safety (5), a majority (50.7%) still agree that verification would reduce free expression. For the group that prioritizes Digital Freedom (1), 70% agree. The data show that, when it occurs, prioritizing safety is a deliberate acceptance of a limitation on free speech, underscoring the need for narrowly tailored policies.



V. Conclusion

Overall, the research reveals a complex tension between online anonymity and accountability. The literature demonstrates that anonymity can contribute to harmful behavior, but identity verification introduces substantial risks related to privacy, data breaches, and misuse of sensitive information. The survey results show that while users recognize the dangers of anonymous misconduct, they also highly value anonymity for privacy, safety, and expression.

Most respondents do not trust social media companies to protect their personal data, yet some would still comply with verification requirements, showing a conflict between personal risk perception and digital platform dependency. At the same time, users overwhelmingly support the continued availability of anonymous accounts, reinforcing the idea that anonymity serves essential social and personal functions.

These findings suggest that policies requiring mandatory ID verification must be approached carefully. Broad verification requirements may reduce harmful online behavior, but they also pose significant security risks and threaten user autonomy. A more balanced approach—using privacy-preserving verification methods and targeted enforcement—may allow platforms to increase accountability without compromising safety or anonymity.

References

Booth, R. (2025, October 9). *Hack of age verification firm may have exposed 70,000 discord users' id photos*. The Guardian. https://www.theguardian.com/media/2025/oct/09/hack-age-verification-firm-discord-users-id-photos

Law, S. (2024). Effective enforcement of the Online Safety Act and Digital Services Act: unpacking the compliance and enforcement regimes of the UK and EU's online safety legislation. *Journal of Media Law*, *16*(2), 263–300. https://doi.org/10.1080/17577632.2025.2459441

Malik, Gaurav. (2024). Biometric Authentication-Risks and advancements in biometric security systems. Journal of Computer Science and Technology Studies. 6. 159-180. 10.32996/jcsts.2024.6.3.14.

Michael J. Moore, Tadashi Nakano, Akihiro Enomoto, Tatsuya Suda, Anonymity and roles associated with aggressive posts in an online forum, Computers in Human Behavior, Volume 28, Issue 3, 2012, Pages 861-867, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2011.12.005.

Sree, Jaya & Damodaram, Dr. (2012). Anonymity And Accountability In Web Based Transactions. Advanced Computing: An International Journal. 3. 10.5121/acij.2012.3217.