# Ethical Implications of Multi-Factor Authentication (MFA) as a Cybersecurity Policy

Nicholas Gray

Old Dominion University

CYSE425W: Cyber Strategy

Dr. Shideh Yavary Mehr

06/30/2025

**Ethical Implications of Multi-Factor Authentication (MFA) as a Cybersecurity Policy**

Multi-Factor Authentication (MFA) is one of the most essential cybersecurity strategies today, as it offers strong user identity verification in an era of increased cyber threats. MFA requires the user to authenticate their identity by presenting two or more separate factors, such as a password, biometric, or one-time code. While organizations understand that MFA helps increase security, the use of MFA has a range of ethical implications for organizations that need to consider, especially related to privacy, user autonomy, and equitable access.

MFA's most explicit ethical advantage is its ability to protect their data and privacy to a better degree because it adds additional protections against unauthorized access (Mostafa et al., 2023). For example, suppose a user implements MFA when using cloud-based services. In that case, it is very likely to decrease the chances of a data breach that exposes sensitive personal or financial information. An organization has an ethical duty to use reasonable steps to protect an individual's data from avoidable harm, such as reasonable access controls like MFA. From this perspective, MFA promotes privacy and security, two key digital rights today.

However, the ethical costs and risks must be considered and the risks accompanying those perceived benefits. One issue is that some forms of MFA, such as biometric authentication, can present serious privacy difficulties. For example, passwords can be changed if compromised, but the same is not true for biometric data like fingerprints or facial scans. If compromised, there is no going back; if it is misused or stolen, the result could be permanent for the impacted user (Choudhry et al., 2024). Given this, the ethical way to use biometrics, as part of MFA, will require extreme restrictions on data storage, clear consent procedures, and full disclosure about how this sensitive data will be stored, handled, and potentially used.

Another ethical concern entails fairness and inclusivity. MFA systems can sometimes produce unintended and unfair disadvantages for groups, such as older users, disabled people, or users without reliable technology like smartphones to receive one-time passcodes (Kamarudin et al., 2024). Suppose an MFA implementation requires multiple devices or technical steps. In that case, it reduces equal access to a digital service, and ultimately, it has become more challenging to use for these and other excluded populations. Ethically, organizations should guarantee flexibility in MFA implementation and, at a minimum, allow greater variety in verifying users as an acknowledgment of the diverse needs of all users.

Additionally, the overall proportionality of MFA must be assessed. Security measures should not be unduly burdensome in a way that disproportionately restricts user agency and convenience. For instance, an MFA process that is too cumbersome could cause a user to become frustrated, which could prompt the user to adopt risky alternatives such as using a backup code and writing it down, or turning off any additional security aspects. While solving the immediate problem, this action subverts the security's purpose (Mostafa et al., 2023). This dilemma emphasizes an ethical responsibility to balance protection with usability and experience.

Ultimately, clear policies and informed consent are essential. The user should understand what data is collected, the purpose of MFA, and how it will be used, stored, or shared. Transparency will help develop trust and help individuals maintain meaningful control of their information (Choudhry et al., 2024).

In conclusion, while MFA is an opportunity for a firm to implement a cybersecurity policy that protects users' digital privacy and security, the moral aspects addressed in implementing MFA plans must address privacy risks, accessibility, and individual autonomy. Organizations with MFA must ensure the multiple factor policy is secure, inclusive,

proportionate, and transparent to the users in respecting the rights of the individuals while defending against cyber-risk.

## References

Choudhry, M. D., Sundarrajan, M., Jeevanandham, S., & Saravanan, V. (2024). Security and privacy issues in ai-based biometric systems. In *AI Based Advancements in Biometrics and its Applications* (pp. 85-100). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781032702377-5/security-privacy-issues-ai-based-biometric-systems-mani-deepak-choudhry-sundarrajan-jeevanandham-saravanan

Kamarudin, N. H., Suhaimi, N. H. S., Nor Rashid, F. A., Khalid, M. N. A., & Mohd Ali, F. (2024). Exploring authentication paradigms in the internet of things: A comprehensive scoping review. *Symmetry*, *16*(2), 171. https://www.mdpi.com/2073-8994/16/2/171

Mostafa, A. M., Ezz, M., Elbashir, M. K., Alruily, M., Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening cloud security: an innovative multi-factor multi-layer authentication framework for cloud user authentication. *Applied Sciences*, *13*(19), 10871. https://www.mdpi.com/2076-3417/13/19/10871