

Digital Self Defense

Ethical Implications

CYSE 452 Cybersecurity Strategy & Policy

Wayne Ricks, Jr

In the physical world, it is a basic human right that people protect themselves in the instance they feel harmed or threatened by an imminent force. Though it is clear to determine the victim and aggressor in a physical scenario, when considering this same right but with a digital setting, the viewpoints as to who the aggressor is and the response the victim should enact becomes indistinct. Ethically speaking, if someone feels as though they have been attacked or threatened, they have a right to self-defense, but it is imperative that people understand the consequences to retaliation without government involvement. While the relationship between the government and the individual's right to digitally protect themselves may be a bit rocky, officials must take into consideration the ethical values on how the government or private entities can implicate these policies without infringing rights such as privacy. The ethical implication of digital self defense focuses on how morality and privacy are enacted towards individual rights, as well as the potential impact towards critical infrastructures and the legality of retaliating.

It is imperative that during the implementation of a digital self-defense policy, government officials, as well as those within public-private entities, should not neglect the rights that each individual has within the cyberspace realm. Digital self-defense provides critical protection for individual rights by enhancing privacy and security, empowering individuals to safeguard their personal information from unauthorized access and cyber threats. According to the Digital Self-Defense Guide, it states that individuals are given empowerment to control their own information, significantly reducing the risk of identity theft and data breaches (KnowledgeFlow 2024). However, these measures can also inhibit rights in certain ways. For instance, the complexity of some tools can exclude those without technical knowledge, as noted in the Springer article on digital self-defense: "The steep learning curve and financial costs can be prohibitive for some users" (Munch 2022). Moreover, while these tools protect privacy, they

can also be misused for illicit activities, posing ethical dilemmas. Balancing these aspects ensures that digital self-defense effectively upholds individual rights without inadvertently causing harm.

When it comes to a policy structured around digital self-defense, and the potential impact it could have on societal groups, digital self-defense provides benefits to each group, along with a couple of drawbacks. Practices such as encryption and secure communication are beneficial to vulnerable societal groups by protecting their data and ensuring their safety from unconsented surveillance and cyber threats (Levi & Gillum 2018). These practices are very common in today's era, but they also have a few notable drawbacks. Individuals that lack the proper resources and/or technical knowledge to implement these measures are at the highest risk of being victimized. In Chapter 2 of the Digital Self-Defense Guide, it states that civil society groups struggle to keep pace with the digital security requirements due limited budgets and technical expertise (KnowledgeFlow 2024). Organizations must be able to give their teams the proper training and long-term strategic goals in order to effectively manage their security, which can be both costly and time-consuming. Additionally, implementing these types of measures can create other challenges towards usability, alienate users, and make routine tasks more complex for entry-level members. The advantages of digital self-defense in terms of empowerment and protection are obvious, but the expenses involved show how crucial it is to provide training that is easily accessible and to improve society's capacity so that everyone can achieve digital security.

A proactive perspective of digital self-defense effectively addresses individual rights by equipping each individual with the proper tools and practices that encourages them to protect themselves in the digital realm. By utilizing practices such as encryption, strong passwords, and

MFA, people can do their part in preventing cyberattacks and unauthorized access. However, those who lack the expertise to implement these practices have the possibility of being excluded, which can result in inequalities throughout the team. Furthermore, law enforcement and other governing bodies must find a proper balance of utilizing these tools to ensure the safety of individual rights and the public. While digital self-defense does uphold individual rights, it is imperative that each strategy undergoes careful consideration in order to determine if it will be effective to all members of society.

References

Levy, J. & Gillum, K. “Tackling Digital Security Across Civil Society (SSIR).” (C) 2005-2024, ssir.org/articles/entry/tackling_digital_security_across_civil_society#.

Munch, L. “Digital Self-Defence: Why You Ought to Preserve Your Privacy for the Sake of Wrongdoers.” *Ethical Theory and Moral Practice*, vol. 25, no. 2, Apr. 2022, pp. 233–48. <https://doi.org/10.1007/s10677-022-10269-w>.

KnowledgeFlow Cybersafety Foundation. “Digital Self Defense Guide: Cybersafety for Personal Safety.” *KnowledgeFlow Cybersafety Foundation*, 7 Oct. 2024, knowledgeflow.org/resource/digital-self-defense-cybersafety-guide.