Summary Post

◄ Initial Post: Death Machines - The Ethics of Autonomous Weapons

Summary Post ►

Display replies in nested form

Settings

Summary Post

by Fahad Abdallah - Monday, 19 May 2025, 7:15 PM

Participating in the discussion on Rogue Services and its questionable business moves encouraged me to consider how technology firms can impact our society based on their values. Rogue Services is a platform that claims it cannot fail, but in reality, it funds and supports activities such as spreading malware and ransomware (Setiawan & Wibawa, 2024). It can be observed that some companies may prioritize profit over acting ethically, legally, and professionally to protect users, organisations, and public trust.

Working with others who had different backgrounds was a valuable part of this learning journey. In particular, Pëllumb Dalipi pointed out that Rogue allows risk to become part of their business and insists that innocent users in critical areas, such as healthcare, must bear the consequences. Due to his point, I now understand that practices that neglect ethics can end up placing both customers and the entire digital community at risk of cyberattacks. Pëllumb added that following or supporting illegal activities online, such as money laundering, can be considered complicity punishable by law in the modern era. Because of his analysis, I could better understand the risks and consequences of not taking action for platforms.

Likewise, Ali Alzahmi explained that Rogue's advertising tricks lead to a long-term loss of public trust. After Ali discussed "Privacy by Design," I began to think more about security and ethics in digital services. I found his point about being upfront with information to be valuable. According to Ali, companies that actively handle cybersecurity problems and help with removals tend to develop a solid reputation and gain users' trust (Patel, 2024). Rogue Services disregards the views of the public and refuses to be accountable, leading to even greater damage.

After reading both comments, I realised that being ethical in computing means paying attention to ethics as well as technology. Following the guidelines of the ACM or BCS, technology companies are expected to minimise harm to users, protect users' data, and remain honest. Rogue Services illustrates how companies' decisions to put profit above ethics can lead to various issues (Neprash et al., 2022). As a result, people using the internet may get hurt, and others might also lose confidence in digital services.

It made me reflect on how government regulations and laws help ensure accountability for companies. Although the Computer Misuse Act and cybersecurity regulations set out proper guidelines, ethical leaders surpass compliance (Tyagi et al., 2024). To prevent harm, companies should practice responsible management, clearly communicate with all stakeholders, and collaborate with those responsible for regulating their industry.

In brief, I learned this week that truly being ethical in computing means doing more than just inventing exciting technology. It requires being committed to people's safety, earning public confidence, and guaranteeing that digital services meet the needs of society. Rogue Services demonstrates the possible problems that can develop when organisations fail to adhere to ethical guidelines. As a result, I feel driven to promote ethical services, making it clear that transparency, user privacy, and accountability are fundamental for achieving company success.

References

Hou, Y., Guo, L., Zhou, C., Xu, Y., Yin, Z., Li, S., Sun, C., & Jiang, Y. (2024). An empirical study of data disruption by ransomware attacks. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering* (Article No. 161, pp. 1–12). IEEE/ACM. Available at: https://doi.org/10.1145/3597503.3639090 (Accessed: 19 May 2025).

Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z., & Nikpay, S. S. (2022). Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. *JAMA Health Forum, 3*(12), e224873. Available at: https://doi.org/10.1001/jamahealthforum.2022.4873 (Accessed: 19 May 2025).

Patel, K. (2024). *Ethical reflections on data-centric AI: Balancing benefits and risks*. SSRN. Available at: https://ssrn.com/abstract=4993089 (Accessed: 19 May 2025).

Setiawan, A., & Wibawa, A. P. (2024). *Pillars of ethics strengthening professional integrity and dignity in the digital* SSRN. Available at: https://ssrn.com/abstract=4935293 (Accessed: 19 May 2025).

Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial intelligence-based cybersecurity and digital forensics: A review. In A. K. Tyagi, S. Tiwari, S. K. Arumugam, & A. K. Sharma (Eds.), *Artificial intelligence for cybersecurity applications* (Chapter 18). Wiley. Available at: https://doi.org/10.1002/9781394303601.ch18 (Accessed: 19 May 2025).

Permalink **Reply**

◄ Initial Post: Death Machines - The Ethics of Autonomous Weapons

Summary Post ►