IOT and Social Media

Ryan Coon

CYB-630

Dr. Hermano Jorge De Queiroz

June 11, 2025

**How the IoT and social media have been affected by cybersecurity over time.**

The Internet of Things (IoT) and social media have faced significant cybersecurity challenges throughout their evolution. Initially, IoT devices lacked robust security features, making them vulnerable to attacks like malware infections and data breaches. As the number of connected devices increased, so did the attack surface, leading to large-scale incidents involving compromised smart home devices and industrial control systems. These vulnerabilities often stemmed from weak default passwords, lack of encryption, and insufficient software updates. Meanwhile, social media platforms have grappled with various cybersecurity threats, including data breaches exposing user information, the spread of misinformation and malicious content, and the exploitation of user accounts for phishing scams or identity theft. Early social media platforms often had inadequate security measures, making them targets for hackers. Over time, platforms have implemented more sophisticated security protocols, such as multi-factor authentication and improved content moderation, but challenges persist. The evolving nature of cyber threats, including sophisticated attacks like social engineering and AI-powered malware, necessitates continuous improvements in security measures for both IoT and social media. The interconnectedness of these technologies further complicates the issue, as a breach in one area can have cascading effects on others.

**Personally Identifiable Information and Its Ethical Use**

The collection of personally identifiable information (PII) raises significant ethical concerns, as it is often not used entirely for ethical purposes. While many organizations collect PII with the intention of enhancing user experience, personalizing services, or improving security, there are numerous instances where this information is misused or inadequately protected. A major issue is the lack of transparency surrounding data practices; many companies do not fully disclose how they collect, use, or share PII, leading to a lack of trust among users. This opacity can result in users unknowingly consenting to data practices that may not align with their ethical expectations. Furthermore, the ethical implications of mishandling PII are profound, as data breaches can expose sensitive information, leading to identity theft and other forms of fraud. The exploitation of PII for profit, such as selling user data to third parties without explicit consent, raises ethical questions about user autonomy and the commodification of personal information. Additionally, the use of PII can lead to discriminatory practices, as algorithms utilizing this data may inadvertently reinforce biases, resulting in unfair treatment of certain groups. Although regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) aim to enforce ethical data handling, compliance is often viewed as a mere checkbox exercise rather than a genuine commitment to ethical practices. In summary, while the collection of PII can be beneficial when handled ethically, numerous factors contribute to its misuse, highlighting the need for organizations to adopt a more responsible approach to data ethics, ensuring that they protect user privacy and use PII in ways that are transparent, fair, and respectful of individual rights.

**Security by Design in IoT Devices: A Costly but Necessary Decision**

As an executive member facing the decision of whether to implement built-in security in our IoT devices at a cost three times higher than the standard model, I would advocate for the investment, aligning my decision with a Christian worldview. The core of Christian ethics emphasizes stewardship, the responsible management of resources and the protection of others. Building security directly into our IoT devices is a manifestation of this principle. It acknowledges the inherent value of the data and privacy of our users, who are created in God's image (Genesis 1:27).

Choosing the more secure option reflects a commitment to protecting the vulnerable. IoT devices, often integrated into homes and critical infrastructure, can be targets for malicious actors. By prioritizing security, we are actively safeguarding our customers from potential harm, such as identity theft, financial loss, or even physical danger. This proactive approach aligns with the biblical call to love our neighbors (Matthew 22:39) and to care for those in need.

While the increased cost is a significant consideration, it must be weighed against the potential consequences of inadequate security. A data breach could result in substantial financial losses, reputational damage, and legal liabilities. Furthermore, the ethical implications of failing to protect user data are severe. The Christian faith calls us to act justly, and this includes protecting the privacy and security of those who trust us. By investing in built-in security, we demonstrate a commitment to integrity and responsible business practices, reflecting the character of God.

**Informing Users of the Risks of Sharing Personal Information**

The digital landscape, while offering incredible opportunities for connection and information sharing, presents significant risks associated with posting personal information. Once information is online, it's nearly impossible to completely remove, potentially leading to long-term consequences. Identity theft is a major concern; personal data can be used to open fraudulent accounts, make unauthorized purchases, or even access financial resources. Furthermore, the information shared online can be used for stalking and harassment, enabling malicious actors to locate and target individuals. Scams and phishing attempts are also prevalent; personal information can be used to trick users into revealing sensitive data or transferring money. Sharing location data can make individuals vulnerable to physical harm or burglary. To mitigate these risks, it is essential to exercise caution and responsibility. Avoid sharing sensitive information on public platforms, be mindful of privacy settings, and carefully consider who you connect with online.

**Privacy Laws and Legal Protection Against Social Media Abuses**

The EU's General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA) are crucial in safeguarding personal data on social media. They mandate explicit user consent for data collection and processing, grant users data access and deletion rights, and regulate data sharing. However, inconsistent enforcement and potential gaps in coverage across all online platforms remain challenges. Therefore, continuous updates to privacy laws are vital to keep pace with technological advancements and ensure robust user privacy protection.

**The Ethical Implications of Cybersecurity Policies**

Cybersecurity policies must strike a balance between protecting intellectual property and user data while upholding privacy rights. Robust security measures, such as encryption and secure data storage, safeguard against unauthorized access; however, they can also raise ethical concerns if they compromise user autonomy. Excessive surveillance or data collection without consent, for example, is a clear privacy violation. Ethical cybersecurity demands transparency, ensuring users understand data collection and usage practices. Policies should prioritize user consent and control, fostering trust and aligning with a Christian worldview of responsible stewardship, thus respecting both security and privacy in the digital realm.

References:

Bruno, B. (2024, August 12). Council Post: Accelerating Fraud Detection With Ethical Use Of Personally Identifiable Information. *Forbes*. https://www.forbes.com/councils/forbestechcouncil/2021/08/26/accelerating-fraud-detection-with-ethical-use-of-personally-identifiable-information/

data.org. (2024, September 23). *Guide: How to respectfully use and inform communities about Personal Identifiable Information (PII) collected about them  - data.org*. Data.org. https://data.org/guides/how-to-respectfully-use-and-inform-communities-about-personal-identifiable-information-pii-collected-about-them/

Dritsas, E., & Trigka, M. (2025). A Survey on Cybersecurity in IoT. *Future Internet*, *17*(1), 30–30. https://doi.org/10.3390/fi17010030

ICS Security. (2018, April 25). *The Importance of Security by Design for IoT Devices*. IIoT World. https://www.iiot-world.com/ics-security/cybersecurity/the-importance-of-security-by-design-for-iot-devices/

John, D., & Sai Monika. (2022, October 17). *The Impact of IoT on Cybersecurity*. https://www.researchgate.net/publication/388454954\_The\_Impact\_of\_IoT\_on\_Cybersecurity

Kaspersky. (2017, September 13). *15 Internet Safety Tips and Internet Safety Rules | Kaspersky*. /. https://www.kaspersky.com/resource-center/preemptive-safety/top-10-preemptive-safety-rules-and-what-not-to-do-online?srsltid=AfmBOoobNaMh3P2TAYXSWuwvu2hl51uEvKFyKm4PkPaA\_DPC\_BZR9g13

Kozhuharova, D., Kirov, A., & Al-Shargabi, Z. (2022). Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them? *Cybersecurity of Digital Service Chains*, *13300*, 202–221. https://doi.org/10.1007/978-3-031-04036-8\_9

Mazhar, T., Talpur, D. B., Shloul, T. A., Ghadi, Y. Y., Haq, I., Ullah, I., Ouahada, K., & Hamam, H. (2023). Analysis of IoT security challenges and its solutions using Artificial Intelligence. *Brain Sciences*, *13*(4), 683. https://doi.org/10.3390/brainsci13040683

NCA. (2025). *Tread Lightly Online: How to Check and Manage Your Digital Footprint - National Cybersecurity Alliance*. Staysafeonline.org. https://www.staysafeonline.org/articles/tread-lightly-online-how-to-check-and-manage-your-digital-footprint

U.S. Department of Labor. (n.d.). *Guidance on the Protection of Personal Identifiable Information | U.S. Department of Labor*. Dol.gov. https://www.dol.gov/general/ppii