**Reflective Portfolio Activities**

**Title of Activities:**

**Unit 1: Ethics in Computing in the Age of Generative AI**

**Unit 5: Inappropriate Use of Surveys – Case Study and IoT Parallels**

**Main Assignment Topic:  
Cybersecurity Threats in IoT in the Government Sector**

**Student Name:  
[Your Full Name]**

**Student ID:  
[Your Student ID]**

**Table of Contents**

[1 Activity 1- Ethics in Generative AI, Linked to IoT Cybersecurity in Government 2](#_Toc210207679)

[1.1 Introduction 2](#_Toc210207680)

[1.2 AI Governance Challenges and Parallels with IoT in Government 2](#_Toc210207681)

[1.3 Tension: National Security vs Civil Liberties; AI and IoT 3](#_Toc210207682)

[1.4 Impact Analysis 3](#_Toc210207683)

[1.4.1 Legal Implications 3](#_Toc210207684)

[1.4.2 Social Implications 4](#_Toc210207685)

[1.4.3 Professional / Ethical Practice Implications 4](#_Toc210207686)

[1.4.4 Conclusion 4](#_Toc210207687)

[1.5 References 5](#_Toc210207688)

[2 Activity 2: Inappropriate Use of Surveys and IoT Parallels 6](#_Toc210207689)

[2.1 References 7](#_Toc210207690)

# Activity 1- Ethics in Generative AI, Linked to IoT Cybersecurity in Government

## Introduction

Generative AI has increased exponentially since 2022, sparking renewed discussions on governance, ethics, fairness, transparency, and accountability (Corrêa et al., 2023; Batool et al., 2025). The existence of many ethical frameworks is not effective due to their fragmented and symbolic application (Díaz-Rodríguez et al., 2023). Other IoT cybersecurity issues can be found in the government, where smart city sensors, defence systems, and medical equipment can make the government more efficient but increase the risk of surveillance by citizens (Saunders et al., 2024). This reflection looks at similarities in AI and IoT governance in the context of national security, civil liberties, and broader impacts.

## AI Governance Challenges and Parallels with IoT in Government

The process of artificial intelligence regulation is associated with permanent challenges, as there is no international consensus on ethical principles and priorities of regulation. According to Corrêa et al. (2023), even though more than 200 ethical principles have been proposed worldwide, there is no unanimity among jurisdictions that inhibits standardisation in such aspects as fairness, accountability, transparency, and others. On the same note, BCS (2023) notes the lack of connection between abstract ethical principles, such as justice, beneficence, and respect of rights and their practical implementation. It is also emphasised by researchers that multi-level governance, balancing the local, national, and international regulatory requirements (Batool et al., 2025) and accountability and independent oversight mechanisms (Mökander et al., 2023), is highly important.

Similar quandaries in the IoT cybersecurity of government systems exist. Diversity in national practices leads to unequal security standards: one type of government focuses on surveillance and control, whereas another one focuses on privacy and protection of citizens (Jha and Jha, 2024). Ethical codes like the Menlo Report establish normative requirements, but the implementation of ethical standards in procurement, maintenance, and monitoring of government IoT devices is rather patchy (Finn and Shilton, 2023). Similarly to the conflict in AI governance mirroring differences in risk and fairness tolerances, IoT governance encompasses the same conflicts about tolerable trade-offs between security, data gathering, and ensuring civil liberties in common systems (Fjeld et al., 2020).

## Tension: National Security vs Civil Liberties; AI and IoT

Generative AI has increased the ethical hazards of profiling, automated decision-making, and abuse of algorithms, which have brought up the issues of proportionality, consent, and justice (Corrêa et al., 2023; BCS, 2023). These dangers are similar to those that have long been discussed in the governance of the IoT in government infrastructures, where national security interests frequently come into conflict with civil liberties. The use of smart cities, surveillance cameras, and connected healthcare systems can help to understand how IoT technologies can make life more efficient and safer, but also provide opportunities to engage in intrusive monitoring (Jha and Jha, 2024). Government IoT data breaches also continue to reveal sensitive citizen data, raising the question of how much governments are willing to go to protect the population by monitoring (Saunders et al., 2024). Researchers believe that security policies will become intrusive as they transition to disproportional protection toward unmonitored mass surveillance (Fjeld et al., 2020). The balancing act is the incorporation of responsibility and control to make sure that neither AI nor IoT technology is used to undermine democratic privileges.

## Impact Analysis

### Legal Implications

Both AI and IoT governance rely on emerging legal provisions aimed at safeguarding personal data and ensuring accountability. In AI, frameworks such as the EU General Data Protection Regulation (GDPR) and the forthcoming EU AI Act mandate explicit standards for consent, transparency, and risk management (Corrêa et al., 2023). For government IoT, these protections extend to citizen metadata and sensitive information collected by smart city infrastructures, healthcare devices, and defence systems (Jha and Jha, 2024). Yet challenges persist around cross-border data flows, state immunity, and lawful surveillance, which often escape rigorous oversight (Fjeld et al., 2020). Current discourse highlights a “new triad” of governance, privacy, cybersecurity, and legal compliance, as inseparable elements of trustworthy systems (ISACA, 2025). This triad is equally critical for IoT, where inconsistent legislation undermines safeguards and increases the risks of misuse by state and non-state actors.

### Social Implications

The social impacts of AI and IoT regulation are evident in the erosion of public trust when technologies are misused. The improper application of generative AI in profiling or decision-making fosters discrimination, while large-scale IoT breaches undermine community safety and privacy (Batool et al., 2025). Trust in government “smart” services is critical; when systems fail, confidence in state capacity and legitimacy diminishes (Saunders et al., 2024). The digital divide further intensifies inequalities, as vulnerable populations are often more heavily surveilled yet less protected (Díaz-Rodríguez et al., 2023). Opacity compounds these risks: AI decisions are perceived as “black box” processes, while IoT devices operate invisibly in everyday contexts. Without transparency and accountability, both AI and IoT risk shifting in public perception from tools of innovation to instruments of social control.

### Professional / Ethical Practice Implications

The ethical considerations within AI and IoT governance in the governmental sector impose a strong ethical liability on the professionals who design, deploy, and manage them. IT practitioners, engineers, and auditors are expected to coordinate their efforts with professional codes like the BCS Code of Conduct, the ACM Code of Ethics, and IEEE principles, which focus on accountability, fairness, and protection of the public interest (BCS, 2023). However, the pressures of politics and institutions put a strain on these ideals to favour efficiency, cost-cutting, or national security at the expense of privacy and ethical protection (Finn and Shilton, 2023). The dilemmas are critical in situations when governments access commercial off-the-shelf IoT devices with lax security or implement AI without any meaningful transparency. This highlights the importance of interdisciplinary management, involving technical skills, ethical scrutiny and legal adherence to guarantee responsible innovation that does not compromise the societal good but satisfies the fundamental rights.

## Conclusion

The parallels between the regulation of AI and IoT cybersecurity within the government show that the two spheres of concern are the same issues of insufficient regulation, ethical dilemmas, and unfair application. Such risks cannot be tackled legally, socially and professionally. In the future, with a focus on maintaining a balance between innovation and democratic principles, the political answer is the combined governance frameworks with accountability, transparency and efficient technical protection.

## ****References****

Batool, A., Zowghi, D. and Bano, M., 2025. AI governance: a systematic literature review. *AI and Ethics*, pp.1-15.

BCS, 2023. *What are ethics in AI? | BCS*. www.bcs.org. Available at: <https://www.bcs.org/articles-opinion-and-research/what-are-ethics-in-ai/>.

Corrêa, N.K., Galvão, C., Santos, J.W., Del Pino, C., Pinto, E.P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E. and de Oliveira, N., 2023. Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns*, *4*(10).

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., De Prado, M.L., Herrera-Viedma, E. and Herrera, F., 2023. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*, p.101896.

Finn, M. and Shilton, K., 2023. Ethics governance development: The case of the Menlo Report. *Social Studies of Science*, *53*(3), pp.315-340.

Fjeld, J., Achten, N., Hilligoss, H., Nagy, A. and Srikumar, M., 2020. Principled artificial intelligence: Mapping consensus in ethical and rights-based approaches to principles for AI. *Berkman Klein Center Research Publication*, (2020-1).

ISACA, 2025. *2025 Volume 6 The New Triad of AI Governance Privacy Cybersecurity and Legal*. ISACA. Available at: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2025/volume-6/the-new-triad-of-ai-governance-privacy-cybersecurity-and-legal>.

Jha, R.K. and Jha, M., 2024. Optimizing E-Government Cybersecurity through Artificial Intelligence Integration. *Journal of Trends in Computer Science and Smart Technology*, *6*(1), pp.67-87.

Mökander, J., Schuett, J., Kirk, H.R. and Floridi, L., 2024. Auditing large language models: a three-layered approach. *AI and Ethics*, *4*(4), pp.1085-1115.

Saunders, M.N., Lewis, P. and Thornhill, A., 2024. Research Methods for Business Students.

# Activity 2: Inappropriate Use of Surveys and IoT Parallels

The 2018 Cambridge Analytica scandal helped to illuminate just how seemingly harmless questionnaires on Facebook were used to gather the personal data of millions of users without their knowledge (Confessore, 2018). The use of this information was then used in targeting political advertising, which manipulated the mind, thus affecting voter behaviour. Even though the case remains a valuable reminder of how the misuse of data, even in situations where the collection was conducted based on the pretence of voluntary participation, may impair not only individual autonomy but also the democratic process, as well.

The same issues can be observed in the sphere of cybersecurity of the Internet of Things (IoT) in government. Smart cities, healthcare systems, and defence infrastructures have IoT devices that collect sensitive information about citizens to enhance efficiency and service delivery (Jha and Jha, 2024). But these systems, when not well secured, offer a chance to spy, control, and violate the trust of the people. The Mirai botnet attack, which was used to initiate massive Distributed Denial-of-Service (DDoS) attacks, using vulnerable IoT devices to target critical services and interrupt essential services, is an example of how vulnerabilities can be used as a weapon (Carr, 2017). In another case, a vulnerability in connected healthcare devices revealed sensitive medical information, which demonstrates the dangers to privacy and safety if governments do not implement strong protections (Park, 2020).

The similarities between Cambridge Analytica and the abuse of IoT are obvious. Surveys in the former and insecure infrastructures in the IoT allow psychological and security and privacy manipulation, respectively. Both take advantage of asymmetries of knowledge: citizens do not know a lot of the time how their data is processed, repurposed or weaponised.

Ethically, both instances can be discussed in terms of personal data misuse with no meaningful consent, which is against the principles of autonomy, beneficence, and justice (Finn and Shilton, 2023). The social effect is also harmful, with the destruction of trust in platforms or government structures weakening trust in the institutions and technology. Both violations are examples of gaps in data protection legally: there are laws regarding data protection, including GDPR, but they are disrupted by intermittent enforcement (Corrêa et al., 2023). IT and cybersecurity professionals have a professional duty to create secure systems, implement protection, and resist pressures leading to the undermining of ethical standards (BCS, 2022). Moreover, IEEE (2020) and ACM Codes of Ethics (2018) emphasise accountability, privacy, and public welfare, reinforcing responsible practices in AI and IoT governance.

Finally, both Cambridge Analytica and IoT abuses reach the same conclusion: responsible technologies are those that do not violate rights and trust. Governments should develop more robust governance systems by making sure that the survey-based platforms, as well as the IoT infrastructure, are constructed and governed with proportionality, transparency, and regulation at their centre.

## ****References****

Association for Computing Machinery (ACM), 2018. *ACM Code of Ethics and Professional Conduct*. Association for Computing Machinery. Available at: <https://www.acm.org/code-of-ethics>.

BCS, 2022. *BCS Code of Conduct | BCS*. www.bcs.org. Available at: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/>.

Carr, M., 2017. The Role of Transnational Expert Associations in Governing the Cybersecurity Risks of the Internet of Things.

Confessore, N., 2018. Cambridge Analytica and Facebook: the Scandal and the Fallout so Far. *The New York Times*. 4 Apr. Available at: <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>.

Corrêa, N.K., Galvão, C., Santos, J.W., Del Pino, C., Pinto, E.P., Barbosa, C., Massmann, D., Mambrini, R., Galvão, L., Terem, E. and de Oliveira, N., 2023. Worldwide AI ethics: A review of 200 guidelines and recommendations for AI governance. *Patterns*, *4*(10).

Finn, M. and Shilton, K., 2023. Ethics governance development: The case of the Menlo Report. *Social Studies of Science*, *53*(3), pp.315-340.

IEEE, 2020. *IEEE Code of Ethics | IEEE*. Ieee.org. Available at: <https://www.ieee.org/about/corporate/governance/p7-8>.

Jha, R.K. and Jha, M., 2024. Optimizing E-Government Cybersecurity through Artificial Intelligence Integration. *Journal of Trends in Computer Science and Smart Technology*, *6*(1), pp.67-87.

Park, Y., 2020. Development and Evaluation of a Security Agent for Internet of Things.