Systems-Theoretic Analysis of Ethics in Computer Science and Emerging Technologies

Anthony J. Coots

National University

TIM-8102: Principles of Computer Science

Dr. *******

June 1st, 2025

Systems-Theoretic Analysis of Ethics in Computer Science and Emerging Technologies

With the rise of technology, particularly in areas related to computer science and emerging technologies, there has been a great challenge in establishing guardrails on what is and is not ethical among new developments. There are both ethical and social issues that arise in technology, including digital privacy, algorithmic bias, misinformation, and others, which continuously challenge developers, policymakers, and society at large.

Technologies such as artificial intelligence, the Internet of Things, and automation, including Robotic Process Automation, illustrate how innovation has outpaced the development of ethical guidelines. These technologies operate within and influence broader systems, a dynamic concept in systems theory that emphasizes the interconnectivity between technical subsystems and other societal subsystems, such as law, education, the economy, and the environment.

The goal of this paper is to explore the ethical and social implications of emerging technologies, evaluate the relevant ethical theories and risks, analyze the relationship between computing and non-computing systems, and consider how ethical concerns shape the thinking behind leadership in computer science.

Ethical and Social Issues in Technology

Ethical and social issues in technology manifest as, but are not limited to, digital privacy, algorithmic bias, and the dissemination of misinformation. It was not until recently that specific commercially available large language models (LLMs) provided the ability to turn off a feature that would train their models, based on users' information as it was provided. Purely as a hypothetical, this does not work for users who work with data that is protected, for example, under the Family Educational Rights and Privacy Act of 1974 (FERPA). In this hypothetical

scenario, we assume a community college employs users who utilize a top commercially available large language model, which, at the time, cannot be turned off during model training, but users wish to enhance their productivity. Suppose users provide the data they work with to an LLM that iteratively trains itself on the data it has been given, in this case, with no option to turn off the training of this model. In such a case, there exists a situation where someone unauthorized to view a student's data inadvertently sees this data, and thus FERPA has been violated. However, the violating user should have had the same right to enhance their productivity as anyone else by utilizing the emerging technology that is artificial intelligence. This clearly outlines both an ethical and a social issue in the technology sector.

Although data privacy is a problem, the scenario, as mentioned earlier, only represents a portion of the ethical and social issues in technology today. Other matters, such as algorithmic bias and misinformation, help address other significant portions of the ethical and social issues in technology, although they are not entirely comprehensive. Artificial intelligence technology is only as good as the data it is trained on and the algorithm supporting it. Sufian et al. (2024) highlight this specific idea as they address the mitigation of algorithmic bias in AI systems related to cardiovascular health. They mention how research has shown the gaps in representation, which is a product of uncollected or unused data in these systems. For example, when a model is trained on images of *X* males, it may underperform on *X* women or individuals from different non-*X* backgrounds.

Lastly, misinformation in emerging technologies, such as artificial intelligence, only exacerbates the erosion of trust and the ethical use of these technologies. The previous example highlighted an ethical and social issue that arises when models are trained only on specific data, and how they fall short in representing diverse groups. There is an entirely different problem:

training a model on data that is incorrect or fabricated to demonstrate something that does not exist, such as a prediction based on this data or the generation of an image or video of an event that never occurred. This is a troubling ethical and social issue that is increasingly evident in the rise of global conflict; however, as these emerging technologies improve, the challenge of distinguishing between accurate information and misinformation becomes even greater. As Montheith et al. (2024) state, a user's understanding of the technology and their online habits are correlated with their ability to combat the spread of misinformation. However, many users do not understand just how wrong these emerging technologies, such as ChatGPT, *can* be.

Ethical Implications of Emerging Technologies and Human Rights

Though it is the social frontrunner, there are a couple more emerging technologies worth mentioning beyond artificial intelligence, such as the Internet of Things and Robotic Process Automation. All of these emerging technologies have been proven to help users complete tasks that previously took a considerable amount of time to complete. For example, with artificial intelligence, such as connectionist AI, when used appropriately, it can generate multiple approaches to a problem that an end user may not have considered otherwise. The Internet of Things utilizes sensors, software, and other devices to relay information over the Internet or a local network, which can replace a system previously managed solely by pen and paper. Lastly, for the scope of this paper, Robotic Process Automation refers to software robots that can mimic the actions of a human worker. All of these can be grouped as new technologies designed to improve efficiency and productivity.

A problem arises from engaging with emerging technologies and their impact on individuals. Alabed et al. (2022) in their study on AI anthropomorphism and the tie between self-congruence and self-AI integration note that one implication of using emerging technology is the

need to be mindful of the psychological impact of humanlike AI. Additionally, the integration of self-AI brings three further implications at the individual, group, and societal levels, including overdependence, digital dementia, and concerns regarding data privacy. This is also true for the Internet of Things and Robotic Process Automation, particularly in terms of concerns about data privacy.

An area where these emerging technologies share a commonality is that they all compute as they receive and encode input, process the data, and decode the output. However, this data processing often challenges human rights. Users are typically presented with lengthy terms of service agreements that they rarely read or fully comprehend, and these documents frequently contain clauses that limit, reinterpret, or waive users' rights to privacy and data ownership.

For instance, biometric data collected by Internet of Things devices, such as heart rate monitors or smart home cameras, may be stored and used to train machine learning models, often without a user's informed consent. When this occurs, users are subject to contributing data sets that are later used by commercial AI systems. If the data is later reproduced or misused by those systems, it represents a significant breach of both data privacy and consent. It undermines users' rights to control their personal information.

Systems Theory and the Interdependence of Technology and Society

Systems theory outlines how subsystems, whether natural, social, technological, or otherwise, are composed of correlative and mutually dependent components, and how these subsystems interact with one another and their environments to form a larger system. Systems theory has a pervasive presence in the lives of many people. For example, how the United States' legislative subsystem comprises related components that interact with other subsystems, such as

the executive and judicial subsystems, to support the larger societal system within the country. The same can be demonstrated for the relationships that exist between technology and society.

The nature of emerging technologies means that the ethical challenges they bring cannot be reduced to individual errors or distinct technical failures. Systems theory, in this instance, uses a broader lens by emphasizing how computing technologies interact with social, legal, and organizational environments. Fraser and Suzor (2025) argue that AI harms arise not from specific technical errors but from the interaction of multiple actors, systems, and environmental conditions in the AI value chain.

For example, in a specific but not necessarily rare occasion, a man took his life after a continued conversation with a generative AI system, Chai. The chatbot's responses were not explicitly programmed to encourage suicide. Yet, the behavior arose from the system's training data and the user's psychological vulnerability, illustrating a complex dynamic between social and technological subsystems. The failure stems from a lack of contextual design, a more-than-anticipated user vulnerability, and either improper or inadequate oversight. Systems theory in this example helps guide the investigation beyond technical fault-finding to analyze the conditions and structures that allowed the harm to occur.

Fraser and Suzor (2025) introduce Nancy Leveson's "safety system" theory, which suggests that safety and ethical integrity must be maintained through the management of system-wide conditions, rather than relying solely on component reliability. The theory recognizes that "error-free" systems can still be unsafe if the sociological and technological environment is poorly managed. Additionally, Fraser and Suzor (2025) introduce Lucy Suchman's theory of located accountability to reinforce understanding of how technologies are developed, deployed, and used within certain contexts (cultural and organizational).

Emerging technologies, such as artificial intelligence, the Internet of Things, and Robotic Process Automation, operate not only as computational tools but also as actors in systems larger than themselves, including healthcare, finance, law, and education, which both influence and are influenced by the dynamics between these systems. The interdependence between computing and non-computing systems becomes especially important when obvious ethical failures can lead to harm, as seen in the Chai incident; any ethical evaluation of technology needs to include system-level thinking to implement these technologies responsibly.

Influence on Programming and Thought Leadership

It is nearly impossible to create a program today that will be bulletproof tomorrow. However, it isn't impossible to consider what is and what isn’t ethical when programming. Creating an open-source solution to ChatGPT, as Fraser and Suzor (2025) discuss with GPT-J, should consider both current and potential future ethical and social issues, particularly in light of past problems. It isn’t without valid and fair reasoning that users want a model that isn't trained with bias; some conversations require addressing both sides to communicate a solution effectively. However, there are certain expectations, especially against having technology reinforce the idea of suicide.

Alfayez et al. (2022) reveal a set of ethical concerns that developers face daily, including topics such as software quality, open-source licensing, and billing practices, which demonstrate that ethical reflection, if not normalized, is becoming normalized in the day-to-day decision-making of programmers. Thought leaders in the field are shifting focus from purely technical competence to designing ethical systems that are fair, safe, and transparent. These systems in the study, however, are often guided by the ACM/IEEE-CS guidelines, which, when used more commonly, become an expectation rather than an option.

Ultimately, ethical programming is not about individual integrity but about creating a professional culture where ethical and social issues are surfaced, shared, and resolved appropriately, thereby setting the bar. As Alfayez et al. (2022) suggest in their study, programmers and thought leaders are actively engaging with questions, and leadership in computer science requires an understanding of programming practice with an emphasis on ethics more than ever.

Theories of Ethics and Risk in Emerging Tech

Three of the main groups of theories involving ethics include consequentialism, deontology, and virtue ethics. All three have rational applications in relation to three emerging technologies: artificial intelligence, the Internet of Things, and Robotic Process Automation. What is ethical has a dynamic relationship with risk, and there are also valuable theories of risk associated with these emerging technologies, such as Risk-Benefit analysis and precautionary principles.

McLeish (1993) defines consequentialism as a doctrine that it is best "to do whatever will have the best consequences." Its application in artificial intelligence is to balance the benefits of efficiency and innovation against harm, such as job loss and bias. In the Internet of Things, this considers the tradeoff between convenience and surveillance. Lastly, in Robotic Process Automation, this would evaluate the productivity gains vs. concerns over job displacement. The approach of consequentialism targets something that evokes a great deal of unknowing fear, being replaced by artificial intelligence or software robots. In contrast, other ethical theories, such as deontology, more directly address duties, principles, character, and integrity, which are central to virtue ethics.

In Deontological ethics (2017), deontology refers to ethics where the rightness or wrongness of conduct is based on the quality of that conduct in relation to established rules. In artificial intelligence, this aims to ensure that artificial intelligence "respects" individual rights such as privacy and consent. With the Internet of Things, devices must not collect or share data without explicit permission. Similarly, systems utilizing Robotic Process Automation must not violate rules or bypass legal protocols, even for the sake of efficiency. Its focus lies more on duties and principles rather than consequences, the opposite of consequentialism.

Lastly, from an ethical standpoint, Garcia (2015) places virtue at the central position in ethics, as Ancient Greek philosophers such as Aristotle, Plato, and Aquinas have eloquently investigated. In totality, among the three emerging technologies listed, virtue ethics encourage developers and organizations to act with honesty, humility, and responsibility, prioritizing long-term thinking over quick wins and profit; the leaders and infrastructure of tomorrow would put moral excellence at the forefront opposed to more immediate themes such as duties and principles or what has the best consequences, to offer philosophy, what is morally excellent can be disputed to not always having the best consequences.

Two major risk theories and frameworks that apply to emerging technologies are the precautionary principle and risk-benefit analysis. The Precautionary principle (2007) shares a similar structure to theory and is therefore considered in this paper. It is an approach to innovations that may cause harm if the science surrounding the matter is inadequate. Thus, precaution is warranted in light of the principle at hand. For artificial intelligence, the principle involves avoiding the deployment of a system where the long-term societal impacts are not well understood, such as autonomous weapons. With the Internet of Things, this manifests as caution

around pervasive surveillance and cybersecurity risks; it is best to be precautionary in the face of uncertainty or unknown risks.

Risk-benefit analysis is a type of analysis that assesses the risks and benefits. Given its elementary nature, it exists in various forms for these emerging technologies. It is a common occurrence in engineering, science, and business when deciding whether to adopt or regulate emerging technology. It is important when considering regulatory frameworks for artificial intelligence.

Case Studies: Artificial Intelligence, Internet of Things, and Robotic Process Automation

Not only does the development of artificial intelligence face ethical and social issues when users are reinforced to act on dark concepts such as suicide, as Fraser and Suzor (2025) found, but the bias embedded in artificial intelligence machine learning models can also be demonstrated using a counterfactual fairness framework, as Moon and Ahn (2025). In their study, they demonstrate that counterfactual evaluation, which involves altering sensitive attributes such as gender to see if outcomes change, can uncover invisible discrimination. The implication is clear, in order to be ethical, artificial intelligence must be both performant and fair.

Second, for the Internet of Things, Schoenherr (2022) highlights how devices are increasingly used in psychographic profiling. By analyzing behavioral traces from devices, organizations gain the ability to infer sensitive personality traits and choices, which are then used to influence behavior, a practice that was exposed by the Cambridge Analytica scandal which was alleged to influence voting behavior in the United States in 2016 (Hinds, Williams, & Joinson, 2020). Cambridge Analytica has since disbanded following the revelation of the situation to the public. Internet of Things devices can form a loosely regulated socio-technical system that challenges privacy norms and user content. Ethical failures in this area are not

necessarily the result of a single bad actor but of systemic weaknesses in regulation, data governance, and informed consent mechanisms.

Lastly, Robotic Process Automation in Human Resource Management appears, at first glance, to be a paradox. Automation may make hiring more efficient and retention more effective, but it may also encode biases. Kadirov et al. (2024) examine in their study how AI-RPA tools in HR automate routine functions, such as resume screening, performance evaluations, and retention analysis, while also introducing risks related to algorithmic bias and data privacy. Without oversight of such a tool, Robotic Process Automation systems may filter candidates unfairly or reinforce discriminatory practices in both hiring and promotions.

Conclusion

The evolution of computer science and emerging technologies can reap significant benefits; however, its' evolution has also demonstrated that, when not well guided by ethics, they can be equally harmful. Ultimately, the path forward requires that ethical considerations become essential for demonstrating competency for computer scientists and technology leaders. A reflection of ethics must be embedded at every level of technological development. The future of ethical computing depends on the collective commitment to systems thinking, transparency, and responsible innovation.

References

Alabed, A., Javornik, A., & Gregory-Smith, D. (2022). AI anthropomorphism and its effect on users' self-congruence and self–AI integration: A theoretical framework and research agenda. Technological Forecasting & Social Change, 182. https://doi.org/10.1016/j.techfore.2022.121786

Alfayez, R., Ding, Y., Winn, R., & Alfayez, G. (2022). What is Discussed About Software Engineering Ethics on Stack Exchange (Q&A) Websites? A Case Study. 2022 IEEE/ACIS 20th International Conference on Software Engineering Research, Management and Applications (SERA), Software Engineering Research, Management and Applications (SERA), 2022 IEEE/ACIS 20th International Conference On, 106–111. https://doi.org/10.1109/SERA54885.2022.9806760

Deontological ethics. (2017). In Encyclopaedia Britannica, *Britannica Concise Encyclopedia*. Britannica Digital Learning. https://search.credoreference.com/articles/Qm9va0FydGljbGU6NDQ4NjQw?aid=102577

Fraser, H. L., & Suzor, N. P. (2025). Locating fault for AI harms: a systems theory of foreseeability, reasonable care and causal responsibility in the AI value chain. Law, Innovation & Technology, 17(1), 103–138. https://doi.org/10.1080/17579961.2025.2469345

Garcia, J. L., A. (2015). Virtue ethics. In R. Audi (Ed.), *Cambridge Dictionary of Philosophy* (3rd ed.). Cambridge University Press. https://search.credoreference.com/articles/Qm9va0FydGljbGU6NDI4ODYz?aid=102577

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). “It wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies, 143*, 102498. https://doi.org/10.1016/j.ijhcs.2020.102498

Kadirov, A., Shakirova, Y., Ismoilova, G., & Makhmudova, N. (2024). AI in Human Resource Management: Reimagining Talent Acquisition, Development, and Retention. *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Knowledge Engineering and Communication Systems (ICKECS), 2024 International Conference On*, *1*, 1–8. https://doi.org/10.1109/ICKECS61492.2024.10617231

McLeish, K. (Ed.). (1993). Consequentialism. In *Bloomsbury Guide to Human Thought* (1st ed.). Bloomsbury. https://search.credoreference.com/articles/Qm9va0FydGljbGU6MTQyODE3NQ==?aid=102577

Monteith, S., Glenn, T., Geddes, J. R., Whybrow, P. C., Achtyes, E., & Bauer, M. (2024). Artificial intelligence and increasing misinformation. The British Journal of Psychiatry, 224(2), 33–35. https://doi.org/10.1192/bjp.2023.136

Moon, D., & Ahn, S. (2025). Metrics and Algorithms for Identifying and Mitigating Bias in AI Design: A Counterfactual Fairness Approach. IEEE Access, Access, IEEE, 13, 59118–59129. https://doi.org/10.1109/ACCESS.2025.3556082

Precautionary principle. (2007). In R. Scruton, *Palgrave Macmillan Dictionary of Political Thought* (3rd ed.). Macmillan Publishers Ltd. https://search.credoreference.com/articles/Qm9va0FydGljbGU6MjQ1OTQ5OQ==?aid=102577

Schoenherr, J. R. (2022). The Wholly Alliance: Psychographics Ethics and the Internet of Things. 2022 IEEE International Symposium on Technology and Society (ISTAS), Technology and Society (ISTAS), 2022 IEEE International Symposium On, 1, 1–8. https://doi.org/10.1109/ISTAS55053.2022.10227096

Sufian, M. A., Alsadder, L., Hamzi, W., Zaman, S., Sagar, A. S. M. S., & Hamzi, B. (2024). Mitigating Algorithmic Bias in AI-Driven Cardiovascular Imaging for Fairer Diagnostics. Diagnostics (2075-4418), 14(23), 2675. https://doi.org/10.3390/diagnostics14232675