Critical Thinking Module 2: Ethical Debt in Software Engineering

Alexander Ricciardi

Colorado State University Global

CSC502: Ethical Leadership in Software Development

Professor: Dr. Steven Evans

January 25, 2026

Critical Thinking Module 2: Ethical Debt in Software Engineering

The term “debt” is often used to describe a financial liability or obligation that must be eventually repaid. In software engineering, it is associated with the idea of technological liability that needs to be addressed eventually, such as the concept of technical debt, which can be broadly defined as “the future costs associated with relying on shortcuts or suboptimal decisions made during software development” (Mucci, n.d., p.1). More specifically, technical debt is the future costs of fixing bugs or refactoring code after deploying a software application. By analogy, the concept of ethical debt within the software development process can be broadly defined as the future costs associated with relying on ethical shortcuts or suboptimal ethical decisions made during the development and implementation of a software application. In more specific ethical terms, it is the future costs incurred when organizations release software without fully considering the ethical implications of its design. This paper examines ethical debt in software engineering through an analogy to technical debt, explaining how ethical debt is incurred and analyzing its impacts and resulting harms through two case studies: Clearview AI’s facial recognition practices and the Dutch childcare benefits scandal.

Understanding Ethical Debt

Ethical debt is the accumulation of unresolved ethical risks embedded within a released software application. This ethical risk can be in the form of biased algorithms, data privacy violations, and software product misuse (Meskarian, 2023). To illustrate how Artificial Intelligence (AI) systems are being developed with ethical debt, Petrozzino (2021) compares the similarities and differences between the concepts of ethical debt and technical debt. Table 1 applies this comparison not just to the development of AI software systems but to software development in general.

Table 1

Conceptual Comparison of Technical Debt vs Ethical Debt

Aspect	Technical Debt	Ethical Debt
Source of Debt	Shortcuts in development, such as poor planning/design, un-refactored code, untested implementations, poor documentation, and quick fixes.	Shortcuts in ethics that ignore bias, privacy, or consent issues.
Manifestation	Bugs, unstable systems, and very efficient systems, resulting in high maintenance costs	Biased, unsafe features, privacy breaches, misuse of data, harm to users, resulting in harm to the public.
Impact on Developers	System failures, higher future dev costs, low-value features, and high operational costs	Reputational damage, loss of user trust, legal fines, infringements of rights
Ultimate Cost Paid By	Organization/developers, extra work to fix issues later.	Often, users or society, notably marginalized groups, face bias, ultimately harming the public
Solutions	Refactoring, better engineering practices, quality assurance, testing	Ethical design and implementation principles, diverse/inclusive testing, transparency, governance. Implement an ethical frame that encapsulates the planning, designing, developing, implementation, testing, and deployment of software applications

Note: The table illustrates a conceptual comparison of technical debt vs ethical debt, comparing their respective sources, manifestation, impact on software developers, who ultimately pay the cost, and potential solutions.

As illustrated in the table, the sources of technical debt are shortcuts in code, untested design, poor documentation, and quick fixes, whereas the sources of ethical debt are shortcuts in ethics that ignore bias, privacy, or consent issues. Notably, the sources of both types of debts are defined as shortcuts. Similar analogies can be applied to the manifestation, impact on developers, and solutions aspects of the debts.

However, a notable difference lies in who ultimately pays for the cost. Technical debt cost is incurred and paid by software developers or companies; on the other hand, ethical debt, although it is incurred by software developers or companies, is often "paid" by users or society, who ultimately bear the consequences by suffering harm from discrimination, exclusion, privacy loss, unfair treatment, or other right violations. This implies that harm from ethical debt does not affect software developers directly; consequently, in certain circumstances, software developers treat it as an afterthought or completely ignore it. However, "the problem with ethical debt is that the metaphorical debt collector comes only after harm has been inflicted" (Fiesler & Garrett, 2020, p.1), meaning that software developers will suffer the impact in the form of reputational damage, loss of user trust, and legal fines, after harm has already been inflicted.

AI Facial Recognition Case Study

One example of ethical debt was Clearview AI's misuse of images of people scraped from the internet (social media, websites) without consent. Clearview AI is a facial recognition technology company based in New York that provides facial recognition tools to law enforcement agencies and private companies across the United States and Europe (Rezende, 2020). By 2020, the tech company had collected a database of over three billion human face images, which were used to train face recognition AI powering their face recognition software (Wang et al, 2024). The database of individual faces, including those of minors, was not only used for training an AI but, in essence, repurposed into an AI tool capable of identifying people from pictures or videos without the individual's consent. Clever AI developers were under pressure to deploy a new and revolutionary security product, but in doing so, they neglected their ethical responsibilities to preserve privacy and protect data.

This negligence resulted in a significant accumulation of ethical debt for Clearview AI. It also raised “critical questions about privacy violations, non-consensual data collection, and lack of regulatory oversight in the private sector” (Wang et al, 2024, p.2), more specifically in the AI software engineering field. Moreover, Clearview AI's privacy infringements violated the rights of individuals to control their own biometric data. In consequence, the tech company was found, by several data protection and regulatory bodies, liable for harming individuals, notably minor by using their likenesses without their consent For example, Canada’s federal Privacy Commissioner determined that Clearview’s indiscriminate scraping of online photos was illegal and violated citizens’ expectations of privacy, Sweden fined police agencies for unlawfully using Clearview’s facial recognition on citizens, and in the state of Illinois, Clearview was sued under the Biometric Information Privacy Act (BIPA) for collecting and using Illinois residents’ biometric identifiers without consent (Wang et al, 2024).

Another concrete example of facial recognition software causing harm due to unaddressed accumulated ethical debt is the wrongful arrest of Robert Williams in Detroit in 2020. Williams was arrested in his home in front of his two young daughters, wife, and in plain view of his neighbors, then Detroit police proceeded to detain him for thirty hours before releasing him (ACLU, 2024). Williams was misidentified by an AI face recognition software as the African American man who stole several watches at a Shinola store in Detroit in 2018. The AI face recognition software was designed by DataWorks Plus, which is one of the largest resellers of facial recognition technology to US police departments (Rivero, 2020). An investigation of Williman’s case and other similar erroneous arrest cases by the Detroit police department revealed that the department had no policy or training on how to properly use face recognition tools.

Additionally, the AI tool was known to have racial bias within the AI algorithms; nonetheless, the developer deployed the AI software. This case highlights how both developers and users of the technology often fail to anticipate how a known "bug," in this case, a bias or error in the facial recognition, especially against minorities, would result in public harm and loss of reputation. In other words, they both chose to ignore the ethical debt accumulated through several years of deployment and usage, which resulted in harm to innocent people jailed and their rights to due process violated. Following lawsuits by civil rights groups, DataWork Plus and the city of Detroit, notably the police department, suffered a significant loss of reputation, resulting in increased mistrust from the public, especially from the African American community.

The Dutch Childcare Benefits Scandal Case Study

The accumulation of ethical debt is not exclusive to the private sector; with the emergence of AI-powered software, ethical debt is being accumulated in unprecedented proportions within the government sector. For example, starting in 2013, the Dutch Tax Authorities used an internally developed AI model based on a self-learning algorithm to generate risk profiles of Netherland's residents to detect childcare benefit fraud (Heikkilä, 2022). The AI model was self-trained on internal tax records and administrative databases from municipalities, Social Insurance Bank (SVB), and the Dutch Immigration and Naturalization Service (Hadi & Altıntaş, 2025). Then the AI model was wrapped within a software platform that was given free rein to profile and flag families who were, in its estimation, committing family allowance fraud. A self-learning algorithm, such as the one used by the Dutch Tax Authorities, is a black box, meaning that even the AI developers are uncertain how the AI comes to a decision, making it difficult to address any built-in ethical issues.

In the case of the Dutch Tax Authorities AI, not only was the model a self-training algorithm, but moreover, parameters such as dual citizens or foreign nations were given significant weight within the training process, creating a situation where the model signal generated risk scores that disproportionately target families with lower incomes or belonging to ethnic minorities. This approach ultimately accumulated an ethical debt, which resulted in an incredible amount of harm to families and a catastrophic loss of reputation and financial consequences for Dutch Tax Authorities. The resulting crisis is referred to as the Dutch childcare benefits scandal or "kinderopvangtoeslagaffaire."

The kinderopvangtoeslagaffaire's consequences from the accumulated ethical debt were dramatic; the harm caused to families was severe and, in many cases, life-altering. For years, the Dutch tax authority, solely based on risk profiles generated by the AI model, ordered thousands of families to pay back years of claims (Rao, 2022). "Tens of thousands of families, often with lower incomes or belonging to ethnic minorities, were pushed into poverty because of exorbitant debts to the tax agency. Some victims committed suicide. More than a thousand children were taken into foster care" (Heikkilä, 2022, p.2). This gross neglect of ethical responsibilities by the Dutch tax authority's software developers resulted in direct violation of human rights, causing significant harm to society. Furthermore, the developer's ethical shortcut of willingly feeding data with weighted family nationality parameters to the self-training algorithm resulted in unlawful and discriminatory profiling, treating nationality as a proxy for ethnicity. This infringed on the basic human right to non-discrimination. The Dutch childcare benefits scandal illustrates that those who bear the costs of ethical debt are often not those who incurred it, allowing those who incurred it, in some situations, to easily disregard harms that do not affect them directly.

Nonetheless, after the harm was already done, the Dutch Tax Authority was significantly impacted by the scandal, resulting in financial penalties and a profound loss of trust. The tax administration was fined by the Dutch data protection agency €2.75 million in December 2021, for unlawful, discriminatory, and an additional €3.7 million fine in April 2022 for years of illegal processing of personal data. Other than the financial impact, the tax administration and, by association, the country of the Netherlands suffer loss of reputation and trust, not only from minorities and its own citizens, but also from other European countries. This was an embarrassing scandal for the country as a whole, forcing Prime Minister Mark Rutte's third cabinet (Rutte III) to collectively resign in January 2021 (Van Den Berg, 2021). This case demonstrates that ignoring ethical debt in government software engineering can have disastrous consequences in the form of social harm, legal penalties, and rework, as the Dutch government had to reorganize the Tax Administration and create a Department for the Coordination of Algorithmic Oversight to oversee the development and implementation of AI applications (AP, 2025).

Consequences of Ethical Debt

As demonstrated by the two case studies, the consequences of ethical debt within software development can cascade through social, legal, and organizational processes. The social consequences impacted real people who suffered harm from privacy invasions, wrongful arrests, ruined livelihoods, and psychological trauma. Furthermore, these harms disproportionately affect often already vulnerable groups such as ethnic minorities. Additionally, these social ethical failures from the software developers diminish public trust in the technology (e.g., AI), in the entities that developed them (e.g., Clearview AI, DataWorks Plus), and in the entities that use the ethically flawed software applications (e.g., Detroit police department, the Dutch Tax Authority).

The most concerning aspect of the social impact is who will ultimately pay the cost of the debt. While the ethical debt is incurred by software developers or organizations, it is often paid by society, which ultimately bears the consequences in the form of significant harm. Although the software developers or organizations may suffer loss of public trust, legal penalties, and rework in the form of reorganizational processes, this cost is paid only after social harm has already been inflicted. This accumulation of ethical debt is often caused by shortcuts motivated by efficiency or expediency. However, the software developer's core ethical failure is failing to embed within their development and implementation of software projects an ethical framework capable of preventing the accumulation of ethical debt.

Conclusion

Similar to technical debt, ethical debt is the accumulation of unresolved ethical risks within software applications. These risks often take the form of built-in biases, privacy violations, and product misuse that originate in developers taking “shortcuts” in ethics. Additionally, unlike technical debt, which is often paid by developers through future rework, the ultimate costs of ethical debt are borne by users and society in the form of discrimination, privacy loss, and human rights violations. Developers, however, may suffer the impact in the form of reputational damage, loss of public trust, and legal fines. The case studies of Clearview AI and the Dutch childcare benefits scandal support it and demonstrate that the consequence of accumulated ethical debt for efficiency or expediency reasons eventually manifests in the form of legal sanctions, public distrust, and catastrophic harm to the public and, more often, to vulnerable individuals and minorities.

Therefore, software developers need to embed their development and implementation projects within an ethical framework to prevent the accumulation of ethical debt and to minimize the risk of causing harm to users and the public. Moreover, with the increasing integration of powerful AI software applications within the private and government sectors, the deployment of this application without ethical safeguards can inflict immense harm on society. Thus, upholding and safeguarding human rights through the implementation of ethical frameworks within software development is not a choice or just an ethical responsibility; it is an ethical obligation.

References

ACLU. (2024, January 29). *Williams v. City of Detroit*. American Civil Liberties Union. https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest

AP. (2025, September 3). *Department for the Coordination of Algorithmic Oversight* (DCA). Autoriteit Persoonsgegevens, https://www.autoriteitpersoonsgegevens.nl/en/themes/algorithms-ai/coordination-of-algorithmic-and-ai-supervision/department-for-the-coordination-of-algorithmic-oversight-dca

Fiesler, C., & Garrett, N. (2020, September 16). *Ethical tech starts with addressing ethical debt*. WIRED. https://www.wired.com/story/opinion-ethical-tech-starts-with-addressing-ethical-debt

Hadi, B. B., & Altıntaş, S. (2025, June). Automated decision-making with AI: An analysis of Dutch Tax Authority practices [Unpublished manuscript]. Tilburg University. https://doi.org/10.13140/RG.2.2.12265.97121

Heikkilä, M. (2022, March 29). *Dutch scandal serves as a warning for Europe over risks of using algorithms*. POLITICO. https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/

Meskarian, M. (2023, September 18). *Navigating the minefield: Technical, ethical, and governance debt in AI/ML and generative AI models*. Medium. https://medium.com/@m.a.meskarian/navigating-the-minefield-technical-ethical-and-governance-debt-in-ai-ml-and-generative-ai-models-fd7fa83861e7

Mucci, T. (n.d.). *What is technical debt?* IBM. https://www.ibm.com/think/topics/technical-debt

Petrozzino, C. (2021, January 03). Who pays for ethical debt in AI? *AI and Ethics, 1*, 205–208. https://doi.org/10.1007/s43681-020-00030-3

Rezende, I. N. (2020, August 13). Facial recognition in police hands: Assessing the "Clearview case" from a European perspective. *New Journal of European Criminal Law, 11*(3), 375–389. https://doi.org/10.1177/2032284420948161

Rivero, N. (2020, June 26). *The little-known AI firms whose facial recognition tech led to a false arrest*. Quartz. https://qz.com/1873731/the-unknown-firms-whose-facial-recognition-led-to-a-false-arrest

Rao, R. (2022, May 9). *The Dutch tax authority was felled by AI—What comes next?* IEEE Spectrum. https://spectrum.ieee.org/amp/artificial-intelligence-in-government-2657286505

Van Den Berg, S. (2021, January 15). *Dutch government quits over "colossal stain" of tax subsidy scandal*. Reuters. https://www.reuters.com/world/dutch-government-resigns-over-childcare-subsidies-scandal-2021-01-15/

Wang, X., Wu, Y. C., Zhou, M., & Fu, H. (2024, July 03). Beyond surveillance: Privacy, ethics, and regulations in face recognition technology. *Frontiers in Big Data*, *7*, 1337465. https://doi.org/10.3389/fdata.2024.1337465