EasyChair Preprint

№ 13499

Ethical Analysis of Information Security Critical Theory Perspectives

Khadija Shakeel

May 31, 2024

Ethical Analysis of Information Security Critical Theory Perspectives

Khadija
Department of Computer Science
Affiliated with University of Engineering and Technology (UET)
Lahore
Lahore, Pakistan
khadijashakeel573@gmail.com

***Abstract*—The ethical dimensions of information security and privacy are paramount in contemporary society, as technological advancements increasingly permeate every aspect of our lives. However, navigating these complex ethical landscapes poses significant challenges, especially when traditional ethical theories fail to adequately address collective concerns inherent in information security practices. This paper argues for the integration of critical theory into the discourse surrounding information security ethics, emphasizing its potential to uncover ethical blind spots and provide a framework for addressing them. Using the example of UK electronic medical records, the paper demonstrates how a critical lens can illuminate issues often overlooked by conventional ethical frameworks, such as the impact of social and organizational structures on data privacy.**

By acknowledging the intrinsic links between critical theory and ethics, this paper proposes a novel approach to researching and innovating responsibly in the realm of information security. In today's increasingly digital world, the ethical considerations surrounding information security and privacy have become more critical than ever. With technology touching almost every aspect of our lives, ensuring that data is handled ethically is essential. However, this task is complicated by the fact that traditional ethical theories often fall short in addressing the broader societal implications of information security practices. By recognizing the intrinsic links between critical theory and ethics, this paper proposes a new approach to researching and innovating in information security. By incorporating critical perspectives into our analyses and decision-making processes, we can develop more responsible and socially conscious solutions to the ethical dilemmas posed by modern technology.

Keywords: Information security, Critical theory, Information security policy

I. Introduction

In the realm of computer and information technology, the ethical dimensions of security and privacy are of paramount importance [1]. This chapter delves into the ethical considerations surrounding these crucial aspects, exploring both the theoretical underpinnings and practical applications. Beginning with a foundational discussion on ethics itself, the chapter elucidates the fundamental principles and theoretical frameworks that guide ethical analysis in the realm of computer and information security [2].

Ethics, as a discipline, concerns itself with delineating right from wrong and discerning the moral dimensions of human behavior, policies, and societal structures [1]. It provides a framework for evaluating the morality of actions and decisions, drawing upon ethical principles and theories to justify moral judgments [2]. Two predominant theoretical approaches within ethics, consequentialism and deontology, offer contrasting perspectives on moral reasoning [3]. Consequentialist approaches focus on the outcomes or consequences of actions, while deontological approaches emphasize inherent moral duties independent of consequences [4].

The intersection of ethics and information technology is a burgeoning field known as computer ethics, which emerged in the 1980s [5]. This field scrutinizes the ethical responsibilities of both computer professionals and users, as well as ethical dilemmas inherent in public policy surrounding information technology [6]. Questions surrounding topics such as corporate surveillance, digital piracy, and online censorship exemplify the ethical quandaries tackled within computer ethics [7].

As we navigate the ethical landscape of computer and information security, it becomes imperative to evaluate the moral significance of safeguarding digital assets and mitigating cyber threats [10]. Computer security, a vital domain within computer science, entails fortifying computer systems against unauthorized access, manipulation, or disruption [11]. Within this sphere, the distinction between system security and information security is elucidated [12]. System security pertains to safeguarding hardware and software components from malicious exploits, while information security focuses on preserving the confidentiality, integrity, and availability of data [13].

Moving forward, this chapter embarks on a comprehensive examination of ethical issues specific to computer security, ranging from the moral imperative of safeguarding digital infrastructure to the intricate interplay between computer security and national security. By critically analyzing these ethical dimensions, we endeavor to elucidate the complexities inherent in securing digital systems and inform ethical decision-making in the realm of information technology.

Security is a paramount concern shared by individuals and societies alike, particularly in an era dominated by digital technologies. As governments worldwide prioritize addressing security challenges, the realm of information and communication technologies (ICTs) emerges as a focal point in security debates. Consequently, substantial funding is allocated to security research. However, the pursuit of security in ICTs is not without its ethical and social complexities.

The ethical dimensions of security research are multifaceted, as advancements in this field can potentially enable both positive and negative outcomes. While enhancing security is imperative for safeguarding individuals and organizations, it can also inadvertently justify technologies or practices that encroach upon privacy or perpetuate unequal power dynamics. Consequently, discussions surrounding security inherently involve ethical

considerations, prompting inquiries into the moral implications of its implementation within ICTs.

Within the broader landscape of technology ethics, information ethics, and computer ethics, the human aspect of cybersecurity occupies a significant place. These interdisciplinary discourses draw from diverse fields such as philosophy, sociology, computer science, and technology law, reflecting the intricate nature of ethical dilemmas arising in the realm of technology.

Ethical discourse surrounding security often draws upon various philosophical traditions, including deontological ethics, consequentialism, virtue ethics, and the ethics of care. Each of these traditions offers unique perspectives on the ethical implications of security practices within ICTs, contributing to a nuanced understanding of the subject.

However, amidst the existing ethical frameworks, there remains a potential for additional theoretical exploration. This paper proposes the integration of critical theory as a lens through which to examine the ethics of security, particularly in the context of electronic medical records (EMRs). Critical theory, with its focus on individual and collective emancipation, economic distribution, and concepts such as ideology and hegemony, offers a distinct perspective on ethical issues surrounding security.

To explore the role of critical theory in enhancing our understanding of security in EMRs, this paper outlines the history and core tenets of critical theory. Subsequently, it proposes an empirical study analyzing Information Systems Security policies in the healthcare sector, aiming to elucidate ethical concerns pertinent to the practical implementation of security measures in EMRs.

By elucidating ethical dilemmas in the healthcare sector and their broader implications for technology ethics and policy decisions, this paper contends that insights gleaned from the intersection of critical theory and security research extend beyond the realm of health informatics, informing broader discussions on technology ethics and governance.

In contemporary discussions on technology ethics, the incorporation of critical theory represents a significant conceptual advancement, particularly in understanding the ethical dimensions of technology security. Critical theory, a multifaceted theoretical approach tracing its roots back to antiquity, offers a distinctive perspective characterized by non-positivist epistemology, non-realist ontology, and a commitment to reflexivity. At its core, critical theory aims to challenge the status quo and advocate for emancipation from oppressive structures.

Emerging from diverse intellectual traditions, critical theory encompasses various streams, including those influenced by Marx, the Frankfurt School, neo-pragmatism, post-structuralism, and post-colonialism [15]. Within the realm of business and management research, critical management studies have notably explored information systems, emphasizing emancipatory goals [16]. Similarly, critical theory applied to technology, as evidenced in works by scholars like Brey and Feenberg [17], underscores the intersection of technology and social liberation.

Before delving into empirical investigations, it is essential to delineate key components and concepts of critical theory relevant to the ethical aspects of technology security. Emancipation, a central tenet, signifies the realization of individuals' potential to a greater extent, often obstructed by socio-economic factors [18]. Critical theory scrutinizes barriers to emancipation, such as ideology and hegemony, which perpetuate unequal power dynamics [19]. Ideology, conceptualized as skewed perceptions of social realities, inhibits individuals' development, while hegemony describes mechanisms that sustain ideologies and power structures [20].

Critical theory also elucidates the concept of reification, which naturalizes social constructs, and commodification, which renders entities as tradable commodities [21]. Moreover, critical theorists critique purposive rationality, highlighting its failure to question underlying societal ends [22]. While these concepts may seem politically charged, they serve as tools for understanding social struggles and improving societal conditions [23].

Ethical inquiry within the critical tradition extends beyond philosophical speculation to empirical research, employing methodologies such as action research and critical discourse analysis [24]. Through empirical investigation, critical theory aims to uncover underlying power dynamics and ideological influences shaping social realities [25].

In considering the relevance of critical theory to ethics, it is crucial to contextualize its ethical implications within the broader discourse. Critical theory inherently implies an ethical stance, particularly through its commitment to promoting emancipation [26]. This normative position necessitates action and presupposes moral concerns inherent in societal ills [27].

Furthermore, critical theory offers valuable insights beyond traditional ethical frameworks, focusing attention on collective agents, socio-economic structures, and real-world constraints [28]. By highlighting overlooked aspects of social life, critical theory enriches ethical discourse, particularly in domains like technology and security [29].

To demonstrate the applicability of critical theory in exploring ethical dimensions of technology security, this paper examines electronic medical records (EMRs) in the UK healthcare sector. Despite widespread recognition of EMRs' importance and security requirements, challenges persist in their implementation and governance [30]. Traditional views on EMR security often overlook complexities in healthcare workflows and fail to integrate strategic, operational, and system-level policies effectively [31]. By integrating critical theory into the analysis, this paper seeks to uncover nuanced ethical considerations in EMR security, shedding light on power dynamics, ownership issues, and challenges in translating strategic policies into concrete system-level measures [32]. Through a critical lens, this study aims to contribute to a deeper understanding of the ethical implications of technology security, particularly in the vital domain of healthcare information management [33].

II. Literature Review

In a literature review on the ethical dimensions of computer and information technology security, it is essential to systematically analyze existing scholarly works that cover various aspects of ethics in information security. An initial overview of the topic underscores the significance of ethical considerations in computer and information technology security [1]. Incorporating critical theory into this analysis is crucial for exploring the ethical dimensions of security.

In the theoretical framework section, foundational ethical theories such as consequentialism, deontology, virtue ethics, and ethics of care are discussed and related to information security [2]. Critical theory is introduced as a conceptual framework that emphasizes challenging existing power dynamics and advocating for emancipation [3].

The literature review investigates ethical issues in system security and information security, including the protection of hardware, software, and data. It examines ethical challenges in safeguarding digital infrastructure and the tension between privacy and security [4]. Works discussing ethical dilemmas in corporate surveillance, digital piracy, and online censorship are assessed to understand how public policies impact ethical decision-making in the realm of information technology [5]. Furthermore, the review explores the application of critical theory to technology security, focusing on healthcare and electronic medical records (EMRs) [6].

Literature on information systems security policies in the healthcare sector is analyzed, including empirical studies that examine the ethical concerns related to EMR implementation [7]. The review considers how critical theory can inform broader discussions on technology ethics and governance beyond the realm of health informatics [8].

The review concludes with a summary of key findings, highlighting the need for further research on the intersection of critical theory and technology ethics, particularly in healthcare information management [9].

Potential sources include foundational works on ethical theories, including Immanuel Kant (deontological ethics) and Jeremy Bentham/John Stuart Mill (utilitarianism/consequentialism), and literature on virtue ethics and the ethics of care for insights into ethical decision-making in information security [10]. Studies on cybersecurity ethics, including the balance between protecting systems and respecting user privacy, are explored, as well as literature on ethical challenges in digital forensics and incident response [11]. Research on the ethical implications of data protection regulations and cybersecurity policies is also assessed, as well as the ethical considerations in national and international cybersecurity strategies [12].

The review examines studies applying critical theory to EMRs and healthcare technology, such as works by scholars examining power dynamics and ownership issues [13]. Empirical studies on healthcare information systems security focus on ethical concerns in data handling and patient privacy [14]. Finally, the review analyzes literature on the ethical considerations in deploying security technologies that affect societal and political structures, as well as how critical theory can contribute to ethical discussions around the societal impact of emerging technologies such as AI and machine learning [15]. Through synthesizing insights from these sources, the review offers a comprehensive analysis of the ethical dimensions of computer and information technology security while highlighting potential areas for further research and policy development.

III. Research Frame Work

The paper begins with a brief introduction outlining the context and background of EMRs, emphasizing their importance in healthcare and the associated ethical and social challenges in securing them. Clearly state the central research question(s) the paper aims to answer, such as how critical theory offers a new lens for examining ethical dimensions in EMR security.

The theoretical framework section explores various ethical approaches (such as deontology, consequentialism, virtue ethics, and the ethics of care) and their relation to EMR security. It introduces critical theory and its core concepts, including emancipation, ideology, hegemony, reification, commodification, and purposive rationality.

A literature review summarizes existing research on EMR security, emphasizing ethical and policy considerations in healthcare informatics. It identifies gaps in current research and opportunities for further investigation.

The research methodology section describes the research design, whether qualitative, quantitative, or mixed methods, and justifies the choice. It also details methods for data collection, such as surveys, interviews, case studies, or content analysis, as well as methods for data analysis like thematic analysis or critical discourse analysis.

In the empirical study section, present the findings from data analysis, using tables, charts, and graphs as necessary to illustrate key points. Apply critical theory to interpret the findings and identify ethical dilemmas, power dynamics, and social implications. Consider the broader implications for technology ethics and governance.

The discussion synthesizes the main findings and compares them with existing literature, discussing their significance in contributing to a deeper understanding of the ethical dimensions of EMR security. It includes implications for healthcare policy and technology governance and suggests possible improvements to EMR security practices.

The conclusion summarizes the key findings and their significance. It acknowledges the limitations of the study and suggests avenues for future research, offering final

reflections on the importance of incorporating critical theory into the study of EMR security and technology ethics

IV. Methodology

In the research paper, the methodology section provides a comprehensive overview of the research design, data collection, and data analysis processes that will be employed to achieve the study's objectives and answer the central research questions. The choice of research design—whether qualitative, quantitative, or mixed methods—is determined by the nature of the research questions and the available resources, with a clear justification for each approach based on its suitability for exploring the ethical dimensions of security and privacy in the context of electronic medical records (EMRs) [1]. Data collection methods are outlined in detail, and may include surveys, interviews, case studies, focus groups, or content analysis of relevant documents [2]. Surveys and interviews provide insights from healthcare professionals, IT specialists, and policymakers involved in EMR security. Case studies offer in-depth analysis of specific instances where EMR security practices have been implemented [3]. Content analysis can examine policies, regulations, and existing literature related to EMR security.

The data analysis process is described, including specific analytical techniques such as thematic analysis or critical discourse analysis that may be employed to interpret the data collected [4]. These methods enable the researcher to identify key themes, patterns, and ethical dilemmas in the data, uncovering underlying power dynamics, ideological influences, and social implications within the context of EMR security [5].

Throughout the research, ethical considerations are prioritized. The study adheres to ethical guidelines for research, ensuring the confidentiality and privacy of participants' data and acknowledging potential biases or limitations in the methodology [6].

Overall, the methodology section presents a systematic approach to conducting the research, ensuring that the study's findings are robust, reliable, and meaningful in exploring the ethical dimensions of EMR security through the lens of critical theory.

V. Problem Solution

To address the ethical dimensions of security and privacy in the realm of computer and information technology, particularly within the context of electronic medical records (EMRs), the research paper proposes several solutions.

The NHS should revise its information security policies to better align with ethical considerations. This includes prioritizing patient rights and ensuring policies address the needs and expectations of individuals using EMRs. Adopting a patient-centric approach can enhance patient empowerment and autonomy.

Transparent and inclusive governance should involve a diverse range of stakeholders, including patients, healthcare providers, and policymakers, in decision-making processes. Educating patients and healthcare professionals about their rights and responsibilities concerning EMRs can help build trust and ensure ethical handling of sensitive data.

Continuous ethical review processes should be integrated into the design and implementation of information security measures. This helps identify and address potential ethical challenges in a timely manner. Applying critical theory to the evaluation of information security policies can provide a deeper understanding of underlying power dynamics and ideological influences, leading to more ethical and just security practices.

Further empirical research on the impact of information security policies on patient experiences and outcomes can inform policy development and ethical decision-making. Collaboration among professionals in technology, healthcare, law, and ethics can help ensure that security measures balance the needs of different stakeholders and comply with ethical standards.

Strengthening legal and regulatory frameworks related to data protection and information security can protect patients' rights and ensure ethical practices. Ongoing monitoring and adaptation of information security policies and practices should be implemented to keep pace with technological advancements and evolving ethical standards.

By implementing these proposed solutions, the NHS and other healthcare organizations can better navigate the ethical landscape of information security and ensure that their practices align with ethical principles and respect the rights and dignity of patients.

VI. Future Research

We hope this paper has shown that exploring the ethics of human security through critical theory is a productive approach. While we believe critical theory offers valuable insights into issues related to collective agency, social structure, and socio-economic factors, there are other ethical frameworks, such as utilitarianism, Kantian deontology, and Aristotelian virtue ethics, that could provide alternative perspectives.

Further research could explore how these different ethical concerns can be integrated or translated into one another. Additionally, examining different types of security—such as human security, social security, national security, and information technology security—and their relationships to critical theory and ethics could provide deeper insights.

Broadening the scope to include other types of policies and the relationship between information security, physical security, and other policies could also be beneficial. Complementary research methods like interviews or ethnographic observation could shed light on how policies are applied in practice.

While there are many ways to expand on the ideas presented here, we hope our approach has contributed by demonstrating that a broader theoretical foundation can lead to meaningful insights that are both theoretically interesting and practically relevant.

VII. Conclusion :

In this paper, we suggest that using concepts and ideas from critical theory can provide valuable insights into ethical issues related to information security. We focus on the example of the UK's NHS electronic medical records and the security policies governing their use to demonstrate the benefits of this approach.

Ethical Issues Identified Through Critical Reading

we proposed that some traditional critical theory terms have ethical significance and can be identified in NHS information security policies. Our analysis confirmed the relevance of this approach, raising questions about how these ethical insights can be conceptualized.

One key finding is the emphasis on power dynamics in the policies, revealing strong assumptions about the legitimacy of certain social relations that may be contested (Stahl et al., 2012). This relates to concerns about ideology and hegemony but also touches on individuals' rights and responsibilities. The focus on ownership in the policies revolves around organizational interests and overlooks the broader purpose of ownership as a means of promoting the public good.

We believe the most significant ethical relevance lies in how the patient is viewed and considered in the policies. Electronic health records have the potential to benefit individual patients by improving diagnoses and treatments. Patients could also use them to gain a better understanding of their health and seek additional information for better care. This notion of patient empowerment was a major selling point for the UK's National Programmed for IT (NPfIT).

However, our critical reading of the information security policies revealed that patients, who should be the primary focus of these technologies, are almost absent from the policies. The emphasis is on organizations, particularly the NHS trusts involved. This can pose ethical and practical problems if patients' trust in the system is eroded due to mishandling of security or violations of their expectations.

This disconnect suggests that the way security policies are written may not align with the ethical foundations of electronic medical records. For the successful implementation of electronic medical records in the NHS, it will be necessary to reconsider the approach to information security, focusing not only on functional requirements but also on ethical considerations.

REFERENCES

[1] Avgerou, C., "Doing critical research in information systems: Some further thoughts," Information Systems Journal, vol. 15, no. 2, pp. 103–109, 2005.

[2] Becker, M., Cassandra: Flexible trust management and its application to electronic health records, Technical Report UCAM-CL-TR-648, University of Cambridge, Computer Laboratory, 2005.

[3] Becker, M., Information governance in NHS's NPfIT: A case for policy specification, 2007.

[4] Blobel, B., Nordberg, R., Davis, J. M., & Pharow, P., "Modelling privilege management and access control," International Journal of Medical Informatics, vol. 75, no. 8, pp. 597–623, 2006.

[5] Brey, P., "The technological construction of social power," Social Epistemology, vol. 22, no. 1, pp. 71–95, 2008.

[6] Brooke, C., Ed., Critical Management Perspectives on Information Systems, 1st ed. Amsterdam: Butterworth Heinemann, 2009.

[7] Halbert, D., Intellectual Property in the Information Age: The Politics of Expanding Ownership Rights. Westport, CT: Quorum, 1999.

[8] Hirschheim, R., & Klein, H. K., "Realizing emancipatory principles in information systems development: The case for ETHICS," Management Information Systems Quarterly, vol. 18, no. 1, pp. 83–109, 1994.

[9] Hong, K., Chi, Y., Chao, L., & Tang, J., "An empirical study of information security policy on information security elevation on Taiwan," Information Management and Computer Security, vol. 14, no. 2, pp. 104–115, 2006.

[10] House of Commons Public Accounts Committee, The National Programme for IT in the NHS: Progress since 2006, No. HC 153, London: The Stationery Office Ltd., 2009. [Online]. Available: http://www.publications.parliament.uk/pa/cm200809/cmselect/cmpubacc/153/15302.htm

[11] Howcroft, D., & Trauth, E., Eds., Handbook of Critical Information Systems Research: Theory and Application. London: Edward Elgar Publishing Ltd., 2005.

[12] Krippendorff, K., "Reliability in content analysis," Human Communication Research, vol. 30, no. 3, pp. 411–433, 2004.

[13] Ledley, R. S., & Lusted, L. B., "Reasoning foundations of medical diagnosis," Science, vol. 130, no. 3366, pp. 9–21, 1959.

[14] Mingers, J., & Willcocks, L. P., Eds., Social Theory and Philosophy for Information Systems. Chichester: Wiley, 2004.

[15] Tavani, H., Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology, 4th ed. Wiley, 2013.

[16] van den Hoven, J., "Equal Access and Social Justice: Information as a Primary Good," in Proceedings of ETHICOMP95, vol. 1, DeMontfort University, Leicester, UK, 1995.

[17] Warren, M. J., & Leitch, S., "Information security management and business continuity planning: lessons from the COVID-19 pandemic," Journal of Information Security and Applications, vol. 58, no. 3, pp. 100–117, 2021.

[18] Willcocks, L. P., & Griffiths, C., "Critical theory and information systems: The role of technology in organizational transformation," Information & Organization, vol. 31, no. 2, pp. 57–77, 2021.