Data Privacy, Ethics and Education in the Era of AI – A University Student Perspective

Rebekah Rousi [1], Hanna-Kaisa Alanen [1,2] and Anne S. Wilson [3]

[1] *University of Vaasa, Vaasa, Finland*
[2] *University of Jyväskylä, Jyväskylä, Finland*
[3] *Deakin University, Melbourne Burwood Campus, Australia*

Abstract

In today's world nothing has been left untouched in relation to artificial intelligence (AI). AI is used for everything from mowing lawns to reporting news. One field in which its presence is highly complex and multifaceted is education. Discussions regarding both the role of AI and the role of learning in education have taken center stage. The field of tertiary education has proven particularly problematic in terms of AI adoption. Ethical issues have arisen across the domain including whether or not generative AI should be used in education and how, the ethicality of learning analytics, and privacy concerns. With the aim of gaining insight into the sentiment of tertiary level students towards privacy in the era of widespread AI, the authors conducted an interview study with nine university student participants. The interviews concentrated on: privacy in studies and student life; data privacy advocacy; level of protection provided by tertiary institutions (universities); understandings of the General Data Privacy Regulation (GDPR); and bodily sensations linked to privacy. The results reveal differences of opinion regarding concern for privacy, yet there was overall consensus that GDPR aided in protection against privacy violation. Findings indicate a tendency towards resignated acceptance and genuine concern for the ethics of university technology-related data practices.

Keywords

Ethics, privacy, higher education, technology, universities, experience, artificial intelligence, trust

1. Introduction

There are no sectors of modern societies that have not been affected by the wide spread implementation and adoption of artificial intelligence (AI). From cooking to surgery, the application of AI-driven systems and machine learning (ML) are either being designed or implemented in ways that transform the ways that services and goods are delivered, as well as the ways in which people work. Along with healthcare, education has been a core field in which the use of AI has been deliberated for the last few decades. Whether early childhood or tertiary education, AI has been considered for a range of use contexts and applications: learning (e.g., virtual tutoring and tailored educational delivery, see [1][2]); learning analytics [3]; grading and feedback; accessibility [4]; facilities management; cooperation and collaboration; as well as safety and security (AI-enabled physical and cyber security systems). Connected to data privacy and trust in the higher educational setting is the idea of organizational trust. Organizational trust refers to the ways in which individuals feel they can trust or depend on an organization to act in a responsible and reliable way, with the individual's interests in mind [5]. There are numerous factors that erode trust such as organizational profits over customer, student or other stakeholder's best interests, manipulation, and lack of transparency – communicating one message while acting in a different way. These are issues that are rife in our current global surveillance society, particularly regarding data privacy and data policy. Universities are organizations in which trust is paramount for the promotion of learning and wellbeing via nurturing psychological safety [6]. Unfortunately, current discussions and advancements on data privacy – the use, collection, storage and trade of personal data (identifiable information such as names, addresses, email addresses preferences etc.) – neglect the impact of

7th Conference on Technology Ethics (TETHICS2024), November 6–7, 2024, Tampere, Finland
Rebekah.rousi@uwasa.fi (R. Rousi); hanna-kaisa.h-k.alanen@student.jyu.fi (H-K. Alanen); anne.wilson@deakin.edu.au (A. Wilson)
0000-0001-5771-3528 (R. Rousi); 0000-0002-8797-3432 (H-K. Alanen); 0000-0001-7369-0258 (A. Wilson)

privacy concerns such a mistrust, stress and anxiety, on the ability to learn within socio-technical environments such as universities and schools. Therefore, in light of current AI developments and data privacy discussions we pose the research question: *How do tertiary students experience data privacy in the context of their university lives?*

The current paper aims to ascertain an understanding of the core concerns university students have regarding data privacy in the context of universities – learning and student life. It explores the relationship between the experience of data privacy, conceptualization of policy and regulation (i.e., in reference to the General Data Privacy Regulation), and higher education. The participants (N=9) were university students (8 females; 1 male) who responded to a text-based interview (qualitative questionnaire) in which they could anonymously and candidly express their feelings and experiences towards matters of privacy in the university context. The study focused on emergent privacy issues in studies and student life, feelings of protection in relation to data privacy, and personal conceptualizations (interpretations) of GDPR among students. The paper begins by describing previous efforts in researching AI and privacy in university settings and among students. The text-based interview method (qualitative questionnaire) is then described in light of participants, procedure, ethical research practices, and analysis. The results are reported according to the question themes, which are subsequently divided into salient themes emerging in the responses. The discussion deliberates the findings in light of the salient themes. Here, new considerations are raised that illustrate the complexity of ethics, privacy and information technology in the university context as a whole.

2. Perceptions of Privacy in Tertiary Education

Issues of privacy at the level of tertiary education have been ongoing for decades. Prevalent issues arising in relation to privacy perceptions of students in higher education institutional settings have included: questions of power and power relations; data (information, knowledge) ownership; policy; vulnerabilities through access to health and performance data; ineffective, inconsistent and unsecure data management practices; and emerging issues related to technological advancements including social media and AI, such as social implications and inaccuracy in predictive algorithms (see e.g., [7][8][9]). Thus, the contemporary tertiary landscape is riddled with traditional concerns related to ownership, security and power dynamics of who has access to what (and whom), combined with the newer complexities introduced by recent advancements in information technology. Coupled with the implementation of automated data-driven systems such as AI, is the rising awareness of privacy matters through policy (i.e., GDPR regulation and practices), scandals (misuse of data and new threats to safety and security, e.g., deep fake fraud), and renewed discussions on agency and fairness in education during the era of AI [10].

The rapid uptake of AI in education that is characterized by formal (i.e., organizational e-learning platforms, learning analytics etc.) and informal (i.e., Large Language Models and generative AI such as Open AI's ChatGPT) adoption has added to interests in delving into issues pertaining to privacy and ethics (e.g., intellectual property, biases, plagiarism and learning etc.). Research articles and discussion papers are growing in numbers as scholars, teachers, administrators and even students alike struggle to grasp the elements, dynamics and impact of AI implementation in specific use contexts. Studies focus on a number of aspects relating to both the education itself, as well as how AI and its ethical implications affect the overall university ecosystem. This demonstrates the complexity of the area, and calls for attention towards gaining detailed insight on a more personal level regarding individual (students', teachers' and other stakeholders) experiences and conceptions across the levels of university involvement. For instance, one study by Irfan, Aldulaylan and Algahtani [10] for instance examined the influence of AI from the perspective of ethics and privacy in Irish higher education. Their findings indicate slight differences in the understanding and perceived severity of data privacy concerns between science and technology-focused students as compared to studies in social sciences, law, public administration and the humanities. They observed that science and technology-focused students harbored greater levels of concern for privacy in the information systems as compared to other students.

Lan Huang [11][11] analyzed the implementation of AI in higher education in light of ethical AI principles identified by the Ministry of Science and Technology of China's "Ethical Rules for New-generation Artificial Intelligence"[12], and UNESCO's *Recommendation on the Ethics of Artificial Intelligence* [13][13]. Huang's study showed a coupling of challenges posed by the increase in mass data collection in universities, with threats to student autonomy and imminent data monopoly. These findings demonstrate longer-term implications for mass data collection at tertiary education level that affect not only individual students and their future lives, but additionally ownership and control of large data sets. These data sets comprise, among other things, intellectual property, identities, learning analytics and predictive models to name some. Other studies such as those by Köbis and Mehner [14][14] and Li, Dhruv and Jain [15], as well as Slimi and Carballido [16] focus more on other ethical questions such as data bias, openness and transparency, trust, human displacement and issues of social-emotional support in AI-enhanced higher education. The issue of privacy once more was raised in terms of future career prospects based on data profiling of students. The current paper probes more into the experiential realm of students – how they have encountered and how they conceptualize data privacy in the context of university studies and university life (the social and life ecosystem surrounding the *student* and university). It delves into issues of trust, safety and the feelings of being protected, while probing understandings of GDPR and what it means to them personally.

Thus, the subjective experience of privacy in the field of tertiary education among students is multifaceted – mingled with personal experiences and diverse understandings of policies, regulations and practices. These sentiments affect not only the experience of learning and *being* on campus and within educational information systems, but play out in other areas of life as ripple effects such as future workplaces, interpersonal relationships, and overall views of trust in society [17]. The consideration of these aspects of privacy in a hands-on creative arts course for non-arts students that ventured through the development and philosophy of photographic technology (from camera obscura to AI and 3D printings) meant that these days commonly discussed issues were embodied, and expressed in non-verbal ways. This makes the current study unique from previous tertiary student privacy research.

3. Method

The study was carried out as a written interview, or open-question (qualitative) questionnaire that was issued to a group of Communication Studies students (N=9) during a workshop course on artistic process with the theme *privacy*. All student participants were of Finnish nationality and were aged between 20 and 50 years of age. The students come from diverse backgrounds – some fresh school leavers in the first and second year of bachelor education, while two were undertaking their second undergraduate degree, re-skilling from other professions. The second-degree students had backgrounds in professional communication and marketing, as well as information technology and e-commerce. The university in question, is traditionally an engineering (particularly energy and software engineering), and business school. Creative practice has not been a part of the formal curriculum in any of the degree programs offered. Therefore, the context of this study was that of a pilot workshop course in art and creative thinking. The students performed exercises designed to increase their sensitivity to the phenomena, the environment, and their own inner voice. The theme of *privacy* directed the students' work and reflections towards a specific phenomenon.

In compliance with GDPR, all students were supplied with information about the study, its purpose and the subsequent publication of results. They were also given a privacy notice stating the type of data that could be collected, where it would be stored, how it would be used, and who would be in charge of storage. Then, in compliance with GDPR and the university's research ethics guidelines, all participants signed an informed consent form. Participants were also made aware of the voluntary nature of the study, which included another part in which they had the option of 'data ownership' and 'attribution of ideas' in which their insight would be made public through privacy-related blogs. All participants agreed to use of their data for the purpose of this study, some (four) agreed to attribution of ideas.

3.1. Procedure

The data for this study was collected via written interview (open field questionnaire) that was issued to the students at the beginning of the workshop course. The questionnaire itself was a part of a sensitization exercise designed to strengthen reflective and embodied awareness of phenomena – in this case, privacy and its relationship to them within their studies and university life. The precise questions are as follows:

Table 1
Interview questions

No.	Question	Description of aim
1	How do issues of privacy emerge within your studies and student life?	Gain an overview of the state of privacy consciousness in university student life
2	Is there any point to advocating data privacy in the era of surveillance economy and machine learning?	Perceived agency in relation to data surveillance
3	What do you feel we're being protected from in relation to data privacy?	Conceptualization of data gathering practices and consequences of them
4	What does the GDPR mean to you? (e.g., as a student)	Perceived level of protection gained from GDPR

As seen in Table 1, the written interview comprised four questions focusing on: privacy issues in studies and student life; data privacy advocacy; the feeling of protection; and conceptualizing GDPR. Another two questions pertaining to bodily feelings of privacy and the boundaries between social curiosity and stalking were also asked. Yet, for brevity sake, we discuss those results in another paper. The study was conducted at the beginning of the workshop course in preparation of delving into the topic at a deeper level through arts-based methods. The study was implemented via Webropol, from which data was stored and processed on excel files. Tables were then constructed and summaries written in Microsoft Word that were then reviewed among the three researchers.

3.2. Analysis

Thematic analysis [18] was undertaken ad hoc (see e.g., [19]) to extract salient themes emerging in relation to the relevant questions. These were then entered into excel. Themes emerging in response to each question were firstly categorized by one researcher, then reviewed by the others. Consensus was made in an iterative online discussion until the researchers were satisfied with the categories. The themes were categorized according to 'approach' (how they approached answering the questions – i.e., personal, general, universal, informative etc.), privacy issue, nature of the privacy issue and examples used within the responses. All three researchers discussed the final results presented in a Microsoft Word document in which summaries and tables were subsequently made. Given the inductive exploratory nature of the study, researchers sought to go beyond the known general concerns of data privacy (i.e., threats of leak, cyber security, misuse of data etc.) and delve deeper into the subjective personal insight of the participants.

3.3. Results

The results present the salient thematic categories of the question responses. The tables explain the approach taken by the participant when identifying and explaining issues. They then note the

perspective of the factor in question, how many participants considered these matters, the nature of the perspective and examples. A total of 22 thematic categories were derived from the responses: privacy issues in studies and student life (eight); data privacy advocacy (six); the feeling of protection (four); and conceptualizing GDPR (five).

3.3.1. The emergence of privacy issues in studies and student life

The responses reveal concern for privacy issues related to digital interaction. These varied in nature between participants (see Table 2). Six out of nine participants approached the question from a purely *personal perspective*. Two participants interpreted it from a more *generic perspective*, and one exhibited *non-recognition* of any privacy issues in relation to their studies or student life.

Table 2
Privacy issues in studies and student life

Approach	Privacy Issues	No.	Nature of Privacy Issue	Examples
Personal	University personal data collection	3/9	Sensitive personal data	Personal information Academic records Library records
Personal	Online university feedback and evaluation	4/9	Confidentiality	Surveys Questionnaires
Personal	Diverse mandatory digital learning platforms	1/9	Confidentiality	Learning platforms
Personal	Academic communication and messaging	1/9	Confidentiality	Emails Social messaging apps
Personal	Participating academic research	1/9	Confidentiality	Thesis research participant
General	Privacy as educational subject	2/9	Privacy-related learning and skills	Communication studies Marketing studies UX design courses
General	Copyright knowledge in social media imagery	1/9	Privacy-related knowledge	IPR laws in visual media marketing
Non-recognition	Absence of privacy awareness	1/9	–	–

The themes arising from the responses are described below. The themes are: university personal data collection; online university feedback and evaluation; diverse mandatory digital learning platforms; academic communication and messaging; participating in academic research; privacy as educational subject; copyright knowledge on social media imagery; and the absence of privacy awareness.

University Personal Data Collection. Two participants expressed their concerns about the university's extensive collection of personal data, which includes, in addition to other personal information, academic records (grades) and other administrative information. One was worried about library records, including borrowed books and research activities, which were considered highly sensitive from a privacy perspective. Another expressed concern for the collected health-related data.

Online University Feedback and Evaluation. Four participants highlighted the importance of maintaining anonymity in online university surveys and questionnaires, where students are highly encouraged to provide, for example, feedback and evaluations. This issue raised the most attention among respondents. The confidentiality was perceived as highly critical.

Diverse Mandatory Digital Learning Platforms. One participant expressed concern for the growing use of diverse digital learning platforms and mandatory digital accounts in usage within education. These accounts necessitate logging in with personal user information. This concern extended to studies in digital environments in general, with particular attention paid to the privacy protection in various group projects. These require collaboration and communication through several platforms, and the privacy was not perceived as trustworthy.

Academic Communication and Messaging. One participant expressed concerns pertaining to emails and other forms of messaging as part of the university student life. This means, for example,

information exchange between students and faculty, encompassing both formal communication and instant informal messaging as well as group discussions through various digital platforms. Increasingly, this kind of messaging may also cover messaging across different locations and time zones due to "remote students".

Participating Academic Research. One participant expressed that privacy-related concerns most commonly arise when participating as a student in various university research initiatives, such as thesis projects. This is an issue that has been addressed in recent times both in university policy across institutions, as well as in ethical research discussions (see e.g., [20]).

Privacy as Educational Subject. Two participants focused on the integration of privacy concerns within their academic learning and course content, thus having a general approach to the question. They highlighted how, in certain areas of their studies, a significant emphasis is placed on understanding and applying privacy-related knowledge and skills. This perspective was seen particularly relevant in fields such as communication studies, marketing studies and user experience (UX) courses, especially considering how marketing and UX design heavily rely on understanding the user, or human dimension in general. Another respondent noted the challenges posed by dark web patterns in UX design.

Copyright Knowledge in Social Media Imagery. One participant highlighted the practical application of copyright laws in the creation and sharing of visuals for student events on social media. This demonstrates an awareness of intellectual property rights in image usage. They were also aware of the social responsibilities involved in creating and sharing content, especially in a public domain like social media. This comes with an understanding of the related ethical and legal considerations within a university student life environment.

Absence of Privacy Awareness. One participant revealed a lack of engagement with privacy issues and an absence of privacy awareness, suggesting that not all students are equally informed of or concerned about these matters. This could also be interpreted as either a relaxed attitude towards privacy or a gap in understanding its significance or value.

3.3.2. Opinions towards data privacy advocacy in the surveillance economy and machine learning

In response to the question of whether there *is any point in advocating for data privacy in the era of surveillance economy and machine learning*, participants collectively acknowledged the complexity of data privacy issues and emphasized the necessity for multifaceted advocacy approaches. All participants unanimously supported the advocacy of data privacy. They highlighted various aspects ranging from viewing *privacy as a fundamental right* to implementing *regulatory strategies and adaptation in digital disruption*, with approaches that were *informative*, *value-based*, *pragmatic* or *forward-looking*. Despite this support, responses from two participants revealed underlying sentiments that questioned the effectiveness of such advocacy, thus expressing *slight skepticism* in an era dominated by surveillance economy and machine learning.

Table 3
Opinions towards data privacy advocacy

Approach	Data Privacy Advocacy	No.	Nature of Privacy Advocacy	Examples
Universal	Unanimous support for data privacy advocacy	9/9	A positive attitude	Important and essential subject Universal need for action
Informative	Promoting data privacy literacy	2/9	Informative education Empowerment	Education on risks Promoting online safety Recognizing data's value in the digital economy

Value-based	Privacy as a fundamental right	4/9	Non-negotiable right	Privacy as a basic principle Upholding individual privacy rights Essential strong data privacy practices Transparency; Trust
Pragmatic	Regulatory strategies and adaptation in digital disruption	1/9	Achieving balance	Creation for reasonable rules and prohibitions to manage the data collection
Forward-looking	Rapid technological evolution and emerging challenges	1/9	Future implications and yet unknown concerns	Rising data privacy issues Potential copyright and identity theft
Slight skepticism	Cautious realism in data privacy advocacy	2/9	Ambivalent sentiments in rapid technological change	Losing the battle Cynicism about the effectiveness

Unanimous Support for Data Privacy Advocacy. All participants support the advocacy of data privacy. This emphasizes the overall affirmative stance of the respondents towards the significance of advocating for data privacy despite the challenges posed by modern technology and data practices. Four participants described the need for advocacy as "important", one as "essential", another as a "basic principle", and one noted that "there is a point" to it. Two participants expressed direct and definitive support by starting their responses with "yes". Overall, these responses indicate that advocating for data privacy is perceived as a critical issue that needs attention. Labelling advocacy as "important" can also be seen as a need for action, implying that it is not just a theoretical concern, suggesting that this is an area where meaningful impact can be made. It might also reflect a sense of responsibility, suggesting an understanding of the broader implications of data privacy for individual rights and societal norms.

Promoting Data Privacy Literacy. Two participants emphasized the relevance of people having a clear understanding of information, data security, and privacy concerns in digital environments, and the importance of being informed about these topics. This suggests the rising significance of digital literacy. One participant expressed concern that people might not sufficiently understand these matters, highlighting the need for educating people about the extent of data collection, its potential uses and risks, and how to stay safe online. Another participant stressed the importance of recognizing data as a valuable asset, or "currency", in the digital economy. This emphasis underlines the need for individuals to be aware of how their data is used and its significance, suggesting that it is worth protecting. Based on participants' responses, advocacy for data privacy encompasses informative education, knowledge gathering, and even empowerment.

Privacy as a Fundamental Right. Four participants shared insights that intertwined the advocacy for data privacy with the belief of privacy as a fundamental right, reflecting a deep connection to values related to personal autonomy and control over one's information. These principles also touch on broader social values and are associated with ethical guidelines, social responsibility norms, cultural values, democratic principles, and human rights standards, for example, that are foundational to societal functioning and governance. One participant described data privacy as a "basic principle," which implies that privacy should be an inherent and non-negotiable aspect of digital usage. Another participant emphasized the importance of upholding individual privacy rights in everyday online interactions, regardless of the digital context, suggesting an awareness of the privacy concerns in routine online activities. One participant argued that the necessity for data transparency and robust privacy practices, especially as digitalization advances, drew attention to the importance of advocating for data privacy.

Regulatory Strategies and Adaptation in Digital Disruption. One participant highlighted the rapid changes and evolution in the digital realm, emphasizing the need for regulatory strategies that are both adaptive and responsive. The participant pointed out the necessity of finding "reasonable rules and prohibitions for gathering and using sensitive information", indicating the importance of

balanced and effective regulation. Additionally, the participant's concern about the potential of "losing this battle" highlights the challenges in regulating a rapidly advancing digital world. This participant also stressed the importance of bridging the knowledge gap in this evolving landscape, suggesting ongoing efforts are essential for protecting privacy in the face of digital disruption.

Rapid Technological Evolution and Emerging Challenges. One participant expressed a direct link between advancements in technology and increased concerns for data privacy. As the participant noted, new technologies, such as AI, bring novel challenges to personal data security, making advocacy in data privacy a dynamic and continually evolving necessity. The participant highlighted specific issues raised by emerging technologies, like voice replication and identity theft through AI, emphasizing the need to keep pace with these transformative technologies. This might include updating laws and regulations to safeguard data privacy and ensuring forward-looking preparedness to address the evolving nature of technology and its implications for privacy.

Cautious Realism in Data Privacy Advocacy. Two participants expressed a certain degree of realism in advocating for data privacy, which may reflect the tone of the question "is there any point". They acknowledged the rapid changes and potential challenges. One participant expressed a belief in losing the battle against the surveillance economy, yet maintained a strong hope for continued advocacy. Another participant conveyed a more skeptical view, expressing "cynicism" about the effectiveness of data protection measures, but still recognized the significance of data privacy efforts. Both responses reflected ambivalent sentiments, combining a mild acceptance of potential defeat with intrinsic optimism and engagement in advocacy for broader benefits.

3.3.3. Feelings of protection in relation to data privacy

Addressing the question, *what do you feel we're being protected from in relation to data privacy,* participants shared a convergence of views, particularly highlighting concerns around *cybercrime, hacking, identity theft and misuse of information.* Seven participants either focused both themes or focused on one, highlighting the significance of these interrelated perspectives. The question also raised the question of personal boundaries and defense, emphasizing the need to shield from manipulation and unwanted influence. Furthermore, three participants specifically pointed out the vital role of organizational institutions in ensuring responsible data privacy protection and maintaining trust.

Table 4
Feelings of protection

Approach	Perceived Protection	No.	Nature of Feeling Protected	Examples
Vigilant attitude	Defense against cybercrime and hacking	5/9	A heightened sense of awareness, a proactive stance	Cybercrime: hacking, data breaches, and digital extortion
Protective	Preventing identity theft and misuse of information	5/9	Desire for comprehensive personal protection	Personal security: shielded from the potential financial losses, personal violations, exploitation, etc. Ensuring autonomy
Defensive	Shielding from manipulation and unwanted influence	3/9	Maintain intimacy, personal boundaries, and emotional security	Defense against manipulative marketing tactics, inundation of misleading content, commercial persuasion

Organizational trust	Academic and organizational trust	3/9	Institutional obligation to protect privacy, thereby enhancing trust	Organizations ensuring academic freedom and fairness, protecting against data misuse and preventing unauthorized access; compliance with laws

Defense Against Cybercrime and Hacking. Participants commonly acknowledged the threat of cybercrime, emphasizing hacking, data breaches, and digital extortion. Four participants specifically focused on these aspects, highlighting the need to safeguard against cyberattacks. This shared view highlights the consensus on the critical importance of securing personal data and preventing unauthorized intrusions, aligning with the broader perception of "being protected from." Additionally, one participant, while not specifically mentioning hacking or cybercrime, emphasized the overarching aim of data privacy protections in shielding individuals from a range of potential harms.

Preventing Identity Theft and Misuse of Information. A significant concern among participants was the prevention of "identity theft," a topic that five participants explicitly highlighted. This concern suggests a need for psychological safety and security in protecting oneself from a broad spectrum of potential harms. Responses also highlighted the risks associated with the misuse of personal information, identity falsifications, and improper use of personal data. Participants emphasized the critical role of privacy measures in providing control over personal information and managing one's digital presence, thereby helping to prevent potential misuse for activities like stalking. Additionally, one participant noted the wider scope of data privacy protections, including safeguarding individuals from financial loss and violations of personal autonomy.

Shielding from Manipulation and Unwanted Influence. Three participants highlighted the significance of regulatory measures, such as requiring consent for marketing, as crucial in empowering individuals to control the information they receive. This stance was viewed as a vital defense against manipulative marketing tactics and the inundation of misleading content. The participants' use of phrases like “try to have influence,” “we are being manipulated,” and “reducing unwanted messages” conveys concerns about external control, deceit, and frustration. These responses reflect not only a concern over the use of personal data but also an increasing awareness and discomfort regarding the exploitation of personal information to influence decisions. Participants' responses suggest an aspiration to maintain intimacy, personal boundaries, and emotional security in the digital sphere.

Academic and Organizational Trust. Participants’ insights shed light on the pivotal role of academic and organizational institutions in protecting individuals from specific privacy-related threats. This corresponds with results obtained in a study by Rousi, Piispanen and Boutellier [5] that observed the willingness to trust publicly funded research institutions in the Nordic countries. One participant emphasized the significance of data privacy in academic settings, highlighting protection from potential repercussions in freely expressing opinions, thereby safeguarding academic freedom and fairness. Another participant emphasized the broader role of secure environments in organizations, indicating protection from the risks of personal data misuse, thereby enhancing trust and safety. A third participant noted comprehensive measures against cyberattacks and data breaches, illustrating how institutions play a crucial role in defending against unauthorized access and ensuring the security of personal information. This also encompasses the assumption of careful compliance with laws.

3.3.4. Personal conceptualizations of GDPR

In exploring the question *what does the GDPR mean to you (e.g., as a student)*, participants shared insights reflecting a combination of *autonomy* and *control*, *assurance*, *legal trustworthiness*, and *personal sentiment of safety*. Overall, responses demonstrated a positive view of the GDPR, with participants appreciating their increased control over personal data and the effectiveness of GDPR rights. They expressed trust that the GDPR ensures privacy, thus aligning with their expectations for

security in daily digital interactions. However, one participant also raised a more realistic view of the risks that come with the presence of digital data, along with a recognition of the limitations inherent in data privacy measures.

Table 5
Conceptualizations of GDPR

Approach	Perspective on GDPR	No.	Nature of GDPR	Examples
Sense of agency	Autonomy and control in informed consent	4/9	Being informed of data use choices, self-governance and personal autonomy	Right to choose to agree or disagree of data use Needed consent
Confidence	Guaranteed privacy and security	4/9	Comprehensive protection	Safeguarding personal information in health, education, and work A tool for empowering privacy rights Protecting against data breaches Ensuring the confidentiality of opinions
Underlying optimism	Regulatory compliance and data responsibility	4/9	Acknowledgment of legal compliance, a sense of responsibility, and trustworthiness	Requirement to follow rules and regulations Control and accountability
Emotional stability	Psychological safety assurance	4/9	Confidence in digital engagement	Safety and trust in the handling and protection of personal data Information is not in wrong hands Safety as a basic need (Maslow's hierarchy)
Realistic	Inevitability of digital footprints	1/9	Challenge in achieving complete data security; acceptance of risks with data presence	Limitations of data privacy measures

Autonomy and Control in Informed Consent. Four participants clearly expressed a sense of agency. They indicated a strong recognition of their rights and an empowerment to actively make informed choices regarding the use and management of their personal data under GDPR. This demonstrates an understanding that individuals are not merely passive subjects of data practices, but active participants with the authority to make decisions about their personal information. The use of terms such as “right to choose to agree or disagree”, “control”, and “consent” highlights the participants’ focus on being well-informed about the data collected from them and possessing the autonomy to consent to or reject how their data is utilized. This highlights the importance of transparency in data handling. Participants reflected that GDPR not only protects data but also provide individuals with psychological comfort about their personal information's safety. Knowing that their data is protected and their privacy is respected under GDPR may reduce e.g., anxiety. For example, safety is one of the basic needs in Maslow’s hierarchy [21], which must be satisfied before an individual can focus on higher-level needs like belonging, esteem, and self-actualization, thus contributing to overall well-being and productivity, and in this case, learning.

Guaranteed Privacy and Security. Four participants clearly highlighted the perceived effectiveness of great GDPR handling in providing a comprehensive shield for individual privacy and security across various personal and professional realms. Their perspectives, while diverse, highlighted the role of GDPR as a defining boundary in data privacy and protection, including enhancing awareness of privacy rights and trust in the systems that manage personal data. One participant stressed the

significance of GDPR in allowing anonymous expression of opinions, thus preventing personal views from unwanted public exposure. Another participant focused on the protection offered by GDPR against potential data breaches, highlighting the security aspects. Further, the recognition of GDPR's comprehensive role in protecting privacy in different life spheres, such as health, education, and work, was noted by another respondent. Additionally, one participant reflected on the increased awareness of individual data privacy rights fostered by GDPR. This suggests participants' sense of confidence and trust in GDPR's ability to protect personal information.

Regulatory Compliance and Data Responsibility. Four participants mentioned the significance of GDPR as a framework for ensuring privacy and security. Among these, two specifically mentioned "rules", highlighting their view of GDPR's systematic regulation as essential for compliance and safeguarding individual privacy rights. The participants' responses indicate an awareness of the need for ethical data handling, involving both individuals and institutions. This draws attention to transparency and accountability, particularly from academic and other formal institutions. Descriptions such as "regulations are to be followed", "rules need to be taken care of carefully", and "required to handle" suggest the participants' trust in the democratic processes and privacy policies, even reflecting loyalty in privacy settings. These responses illustrate how GDPR reinforces personal autonomy in a surveillance economy. The focus on adhering to GDPR regulations and its role in promoting ethical data practices further demonstrates the participants' optimism about GDPR's ability to create a secure and responsible digital environment.

Psychological Safety Assurance. Four participants' responses illustrated the profound meaning of GDPR on individuals' psychological well-being, providing an assurance of safety and trust in the handling and protection of their personal data. Three participants used the word "safe", which suggests a provision of mental and emotional security. Two participants expressed "feel safe" and another one mentioned that GDPR "creates trust that my information is safe and not in wrong hands", indicating a sense of protection against potential digital threats, and presumably also a sense of relief. One participant also pointed out a sense of long-term security and protection against unforeseen data misuse.

Inevitability of Digital Footprints. While the prevailing attitudes towards GDPR among the participants were characterized by trust, one participant offered a more nuanced, realistic perspective. This participant recognized the inevitability of digital footprints and the inherent challenges in achieving complete data security. This viewpoint aligns with findings from previous research [22], which underline that, despite GDPR protections, companies still manage to collect various types of user data. According to the study, this includes volunteered, observed, derived, and acquired data, as well as metadata. This last category, metadata, essentially represents 'data about data', detailing how the other types of data are processed and managed. The participant's response indicates a level of acceptance of the risks associated with digital data presence, merged with an awareness of the limitations of data privacy measures, while choosing not to be overly anxious about it.

4. Discussion

Based on the diverse responses, it became evident that issues related to privacy in studies and student life within the university environment are omnipresent at multiple levels. These issues encompass both formal academic settings and informal aspects of student life, all of which intertwine in digital interactions. The varied responses likely reflected the respondents' initial thoughts when asked about the topic. However, all the themes that emerged were ones that affect every student in one way or another. Additionally, while not explicitly outlined in the responses, they hinted towards a grey area where personal devices (such as computers and smartphones) and university privacy policies might not consistently align. For instance, communication often takes place via personal messaging services operated by large international companies often based outside the European Union. The varied responses highlighted the most crucial aspect: the pervasive nature of privacy concerns in the university setting, influencing both academic studies and everyday student life, and the complex interplay between individual, institutional, and societal factors in shaping perceptions and concerns about privacy. Concerns about data handling, for example, highlighted the socio-cultural dimensions of digital literacy and privacy awareness among students.

While the responses did not explicitly convey strong emotional or affective dimensions, they revealed some underlying sentiments and tones of concern. This was evident in the emphasis on the importance of privacy in research and surveys, the handling of academic records, and communication privacy. The mention of anonymous feedback indicated an expectation for a safe space for honest expression without repercussions, suggesting a cultural norm where open, critical feedback might be socially sensitive. Respondents appeared aware of and concerned about the potential risks and implications of privacy breaches. For some, particularly those discussing the use of digital platforms and uncertainty about data storage and usage, there seemed to be a sense of discomfort, inferred from their concerns about not knowing where data is stored, who has access to it, and its future uses.

In cases where respondents stressed the need for permissions in social media and the handling of academic records, there was an implicit trust that these measures would ensure privacy and security. However, this also suggested a reliance on external systems and policies to safeguard their personal information. Furthermore, in responses focusing on marketing studies, UX design, and university data collection, there was a critical awareness of how privacy issues can affect individuals. This awareness might be accompanied by a concern for ethical practices and the potential emotional impact of privacy breaches. Overall, the responses indicated students' expectations that their privacy be protected in the study context and handled responsibly and confidentially. This also assumed that the university and its administrators act responsibly to protect sensitive information, ensuring safeguards against unauthorized access or misuse.

The participants' responses to the question of advocating for data privacy in the surveillance economy and machine learning era showcased a diverse yet primarily optimistic attitude. Despite mild skepticism from two respondents, the predominant sentiments included optimism, hope, and a strong motivation relevant to supporting data privacy advocacy. These views, while grounded in a realistic understanding of the challenges, also reflected a belief in the potential for positive change amidst rapid technological evolution. This mindset reflected a conscious motivation to improve data privacy protections, acknowledging the broader socio-cultural implications of this issue. Their ambition for robust data privacy practices and effective regulation signaled a desire for tangible improvements in data management and safeguarding. Their commitment to the principles of data privacy suggested a deep, personal engagement with the cause. This emotional stance highlighted the importance of advocating for and believing in the significance of data privacy. Furthermore, the concern about the average person's understanding of data privacy issues touched on the socio-cultural dimension of the digital divide, indicating the need for advocacy efforts that are inclusive and accessible to all. Collectively, the participants' responses demonstrated a belief in the power of both individual and collective action in shaping the discourse on data privacy. They emphasized the importance of understanding and informed participation, positioning individuals as capable contributors to this critical conversation. Notably, the varied perspectives on advocacy highlighted the multifaceted nature of data privacy in the digital era.

In response to the question about feelings of protection and expectations in the context of data privacy, participants revealed a shared understanding of the need for security against various threats, including cybercrime, hacking, identity theft, misuse of information, and manipulation. These indicate the intricate nature of data privacy concerns and the importance of implementing protective measures for psychological safety and personal autonomy. Participants anticipated proactive steps against these threats, signaling a demand for reliable data protection policies. They emphasized the overarching goal of shielding individuals from various potential harms, reflecting a proactive stance in protecting personal data and maintaining control over one's digital identity. The participants' views also demonstrated an increasing awareness and unease about the exploitation of personal information. Additionally, their responses revealed emotional dimensions across the themes, with underlying concerns ranging from fear and vulnerability (cybercrime, hacking), to frustration and discomfort (manipulation, unwanted influence). This suggests a desire for reassurance in the protection of personal autonomy and boundaries, reflecting the importance of sensitive personal information. Expectations extended to the societal role of organizational institutions in maintaining data privacy standards, highlighting how privacy is perceived and managed in broader societal contexts.

Many participants agreed that GDPR offers a significant degree of personal control over data, an essential aspect for students in managing their personal information. This highlights a keen

awareness and appreciation for the rights and protections provided by GDPR, particularly in the context of informed consent and the management of personal data. The sentiment underlying the participants' views was predominantly one of satisfaction and confidence, albeit not overly emotional but rather pragmatic. This suggests a mature understanding of the implications of GDPR in their lives, viewing it as a tool that empowers them with agency and autonomy over their personal data. The emphasis was not just on the systems' abilities to protect data but also on a broader trust in data governance and privacy policies. This trust includes faith in the commitment of organizational institutions upholding ethical practices and responsible data management.

Participants' responses indicate that GDPR has had a positive impact on their public confidence. By being better informed and having control over their personal data, participants felt safer in their interactions within the academic sphere. This sense of safety is not just internal but also extends to their trust in governance systems and legislated laws. The discussions around GDPR highlighted a nuanced understanding among students of their digital rights and privacy. It revealed how GDPR has become intertwined with their daily lives, influencing their perception of personal data control, trust in institutions, and the relevance of privacy in their educational endeavors. The responses reflected a blend of satisfaction with the current state of affairs and a pragmatic approach towards data privacy, emphasizing the importance of personal agency, emotional well-being, and an increased awareness of digital privacy issues, even one participant expressed calm awareness of inevitability of digital footprints.

The study had several limitations. Firstly, the small and relatively homogenous sample size prevents the authors from making any generalizations. Furthermore, more attention should have been given to the demographics of the participants including gender[23], as previous studies have shown that gender plays a role in the way people perceive and are concerned about privacy matters (see e.g., [24][24]). This would be worthwhile testing, particularly in a large-scale quantitative survey. As several of the findings in this study are novel, i.e., concerning the issues of feedback, multi-device and platform utilization in communication and university learning tasks, and concern for the learning environments students are forced to interact with, the emergent categories should be tested for construct validity.

This work provides a platform for future studies specifically focusing on the interaction of personal experience, ethics and data privacy concerns in higher education settings. As AI becomes even more infiltrated in the learning environment, i.e., via digital humans (generative AI created human-like conversational agents), robotics and extended reality, the concerns posed now, may transform into substantial problems in the future. The current study is one part of two larger projects investigating the personal embodied experience of privacy in diverse contexts of pervasive computing. The results presented here are being used as the basis of a framework that explains the complex interaction between policy, practices and personal experience of privacy, aimed to enhance the design of socio-technical systems from the perspectives of ethicality, fairness, and safety.

Acknowledgements

The authors of this paper would like to acknowledge the funders of the research, the Research Council of Finland for its support of the "Emotional Experience of Privacy and Ethics in Everyday Pervasive Systems (BUGGED)" (decision number 348391) and the "Multifaceted Ripple Effects and Limitations of AI in Work, Business and Society (SYNTHETICA)" (decision number 358714), as well as the European Union's Horizon 2020 research and innovation programme, within the OpenInnoTrain project under the Marie Skłowdowska-Curie (grant agreement no. 823971).

Declaration on Generative AI

The authors have not employed any generative AI tools.

References

[1] W. Holmes, I. Tuomi, State of the art and practice in AI in education, Europ. J. of Edu., 57.4 (2022): 542-570. doi: 10.1111/ejed.12533

[2] R. Luckin, W. Holmes, Intelligence unleashed: An argument for AI in education. Pearson Education, 2016.

[3] S.J.B. Shum, R. Luckin, Learning analytics and AI: Politics, pedagogy and practices, Brit. J. of Edu. Tech. 50 (2019). 6: 2785-2793. doi: 10.1111/bjet.12880

[4] E. Goldenthal, J., S.X. Liu, H. Mieczkowski, J.T. Hancock, Not all AI are equal: Exploring the accessibility of AI-mediated communication technology, Comput. in Hum. Behav. 125 (2021): 106975. doi: 10.1016/j.chb.2021.106975

[5] R. Rousi, J.-R. Piispanen, J. Boutellier, I trust you Dr. Researcher, but not the company that handles my data–trust in the data economy (2024), 57th Hawaii international conference on System Sciences, HICSS 2024, Hilton Hawaiian Village Waikiki Beach Resort, Hawaii, USA, January 3-6, 2024. ScholarSpace 2023, ISBN 978-0-9981331-7-1. URL: https://hdl.handle.net/10125/106941

[6] A. Curzon-Hobson, A pedagogy of trust in higher learning, Teach. in Higher Edu. 7. 3 (2002): 265-276. doi: 10.1080/13562510220144770

[7] Y. Tao, W. H. Wang, Fair privacy: how college students perceive fair privacy protection in online datasets, Information, Comm. & Soc. 26. 5 (2023): 974-989. doi: 10.1080/1369118X.2023.2166361

[8] M. Brown, C. Klein, Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents, The Journal of Higher Education 91. 7 (2020): 1149-1178. doi: 10.1080/00221546.2020.1770045

[9] A.J. Braunack-Mayer, J.M. Street, R. Tooher, X. Feng, K. Scharling-Gamba. Student and staff perspectives on the use of big data in the tertiary education sector: A scoping review and reflection on the ethical issues. Rev. of Edu. Res. 90. 6 (2020): 788-823. doi: 10.3102/0034654320960213

[10] M. Irfan, F. Aldulaylan, Y. Alqahtani, Ethics and privacy in Irish higher education: a comprehensive study of artificial intelligence (AI) tools implementation at University of Limerick, Glob. Soc. Sci. Rev., VIII (2023): 201-210. doi: 10.31703/gssr.2023(VIII-II).17

[11] L. Huang, Ethics of artificial intelligence in education: Student privacy and data protection. Science Insights Edu. Frontiers 16. 2 (2023): 2577-2587. doi: 10.15354/sief.23.re202

[12] Ministry of Science and Technology of China, Ethical rules for new-generation artificial intelligence (2021). URL: https://cset.georgetown.edu/publication/ethical-norms-for-new-generation-artificial-intelligence-released/

[13] UNESCO, Recommendation on the ethics of artificial intelligence (2021). URL: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics

[14] L. Köbis, C. Mehner. Ethical questions raised by AI-supported mentoring in higher education. Frontiers in Artificial Intelligence 4 (2021): 624050. doi: 10.3389/frai-2021.624050

[15] ZX. Li, A. Dhruv, V. Jain, Ethical considerations in the use of AI for higher education: A comprehensive guide, in: Proceedings 2024 IEEE 18th international conference on Semantic Computing (ICSC), pp. 218-223. IEEE, 2024. doi: 10.1109/ICSC59802.2024.00041

[16] Z. Slimi, B. Villarejo Carballido, Navigating the ethical challenges of artificial intelligence in higher education: An analysis of seven global AI ethics policies, TEM J. 12. 2 (2023). doi: 10.18421/TEM122-02

[17] J. Polonetsky, O. Tene, The ethics of student privacy: Building trust for ed tech. International Rev. of Inform., Ethics 25 (2014). URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2628902

[18] V. Braun, V. Clarke, Thematic analysis. American Psychological Association, 2012.

[19] B. Adams, G. McKenzie, M. Gahegan, Frankenplace: interactive thematic mapping for ad hoc exploratory search, in: Proceedings of the 24th international conference on World Wide Web, pp. 12-22. ACM, 2015. doi: 10.1145/2736277.2741137

[20] L. Shi, Students as research participants or as learners?, J. of Acad. Ethics 4 (2006): 205-220. doi: 10.1007/s10805-006-9028-y

[21] A. Maslow, Motivation and Personality, second edition. Harper and Row, 1970.

[22] A. Bowyer, J. Holt, J. Go Jefferies, R. Wilson, D. Kirk, J.D. Smeddinck, Human-GDPR interaction: practical experiences of accessing personal data, in: Proceedings of the 2022 CHI conference on Human Factors in Computing Systems, pp. 1-19. ACM, 2022. doi: 10.1145/3491102.3501947
[23] M.G. Hoy, G. Milne, Gender differences in privacy-related measures for young adult Facebook users, J. of Interact. Advert. 10. 2 (2010): 28-45. doi: 10.1080/15252019.2010.10722168
[24] G. Bansal, M. Warkentin, Do you still trust? The role of age, gender, and privacy concern on trust after insider data breaches, ACM SIGMIS Database: the DATABASE for Advances in Information Systems 52. 4. pp. 9-44. ACM, 2021. doi: 10.1145/3508484.3508487