Proceedings of the 11th World Congress on Electrical Engineering and Computer Systems and Sciences (EECSS'25)
Paris, France - August, 2025
Paper No. CIST 114
DOI: 10.11159/cist25.114

Content Analysis of Students' Comments on Utilized Privacy Teaching Methods

Marija Kuštelega[1], Renata Mekovec [1]
[1]University of Zagreb Faculty of Organization and Informatics
Pavlinska 2, Varaždin, Croatia
marija.kustelega@foi.unizg.hr; renata.mekovec@foi.unizg.hr

Abstract **-** In today's digitally linked environment, technology has a significant impact on education. While the advantages are obvious, the rising dependence on digital technologies presents serious privacy problems for students. To examine the perception of the third-year undergraduate students at a Privacy and personal data protection course, regarding utilized teaching methods, 31 students were asked open-ended questions. The objective of this study was to analyze the perspectives of students on the instructional methods that were employed to teach topics that are related to privacy. The student responses were analyzed using the content analysis method performed by QDA Miner Lite software. From the positive aspects, the categories "Excellent teaching organization" (37,50%), "Quality teaching materials" (15,60%), and "Interesting and interactive lectures" (12,50%) had the highest frequency of appearance. On the other hand, as negative aspects, students emphasized: "More real-time examples" (3,10%) and "Lack of time for discussion" (3,10%) as the main places for advancement. The results show that a student-centered approach has proven to be a very effective method in teaching privacy-related subjects.

Keywords**:** content analysis, privacy teaching, students, privacy concerns

1. Introduction

Respecting data subjects and their privacy is crucial for digital trust. Given the increasing value customers place on privacy and the severe consequences of data breaches – including hefty fines, reputational damage, and erosion of trust – the role of privacy professionals is paramount. According to Gartner [1], security and risk management (SRM) leaders responsible for privacy face a growing list of challenges. Customer expectations for privacy are rising, regulatory scrutiny is intensifying, and the C-suite demands the responsible and profitable deployment of AI technologies. By prioritizing privacy and providing adequate resources, enterprises can empower their privacy teams to effectively safeguard data and achieve their broader business objectives [2].

Data privacy professionals face an increasingly complex and evolving landscape, driven by the rise of AI and the continuous changes in regulations, requiring them to constantly adapt their roles and responsibilities. According to a new ISACA report, the long-standing privacy skills gap is now posing a serious security risk, as a lack of training, and failure to detect personal data are all contributing to an increase in data breaches. Therefore, there will likely be a greater need for privacy specialists, with technological privacy roles expanding more quickly than legal/compliance ones [3]. ENISA's assessment of cybersecurity threats for 2030 highlighted a critical skill shortage, ranking it as the second most important challenge [4]. The current status of the global economy has led to reductions in both the number of employees and the budget. The number of people needed globally to adequately secure organizations has increased, but employers are cutting back on hiring and professional development of their privacy and security teams. In the 2024 ISC2 Cybersecurity Workforce Study nearly 60% of participants agree that the absence of skills has had a significant impact on their ability to safeguard the organization, with 58% believing that it poses a significant threat to their organizations [5].

Privacy-related jobs cover names like Privacy officer, Privacy compliance officer/compliance officer, Compliance manager/Privacy compliance manager, Privacy leader, Data protection officer, Data privacy manager, Program manager/Privacy program manager, Privacy analyst, Privacy specialist, Cyber legal advisor and there is no unified description what their key tasks are. There are some frameworks that define competences needed for performing tasks connected to privacy protection, like The European Cybersecurity Skills Framework (ECSF)[6] and NIST Privacy Framework [7]. According to NICE Framework Components [8] — Work Role Categories, Work Roles, Competency Areas,

and Task, Knowledge, and Skill statements work role Privacy compliance is described as role responsible for establishing and supervising the privacy compliance program and personnel of an organization, including the development and management of privacy-related governance, policy, and incident response requirements. Privacy officer/privacy compliance manager should have knowledge in various domains such as cybersecurity operation policies and procedures, information privacy technologies, computer networking protocols, risk management processes, cybersecurity laws and regulations, system threats and system vulnerabilities. Privacy officers should also have skills in developing instructional materials, developing policy plans, aligning privacy and cybersecurity objectives, identifying network threats, performing risk analysis, and creating privacy policies.

The need for effective teaching methods for privacy-related subjects is crucial, as it requires a deep understanding of complex domains and is interconnected with other important sectors/domains like technology, legal rules, and safeguarding user rights. The increasing demand for privacy professionals and the complexity of modern cyber threats underscore the importance of well-designed educational programs. These programs are critical for equipping future experts with the necessary skills and knowledge to effectively navigate this challenging landscape.

Teaching and learning are dynamic processes that require continuous adaptation to new opportunities and challenges. Multiple elements, including student and teacher qualities and attitudes, motivation, and learning environment, among others, interact to affect the quality of student learning at a given moment and under certain conditions [9].

The use of student-centered learning is becoming more and more apparent in privacy and security education [10-13]. Student motivation is essential for creating a positive learning environment; however, teachers often overlook this aspect of students' learning processes, focusing instead on doing the subject [14]. Student-centered teaching strategies like discovery learning, problem-based learning, and case-based learning, are suitable strategies for dynamic content courses like security courses, as it allow students to explore topics on their own or with minimal teacher guidance [15]. Discovery learning, also known as inquiry-based learning, encourages students to develop skills through discovery, focusing on understanding concepts rather than memorizing information [16-17]. Such a learning technique is crucial for preparing future generations to handle challenges that will necessitate the ability to do independent research and solve problems [18]. Problem-based learning seems to be beneficial for developing critical thinking and creativity [19], which is why it is considered the best approach for teaching security courses [13]. Problem-based and case-based learning are both effective deep learning techniques that help build a meaningful connection between theory and practical application [20]. Other types of learning strategies like case-based learning can encourage student discussion and debate [21], but its effectiveness depends on students' preparation prior to the class [15]. Project-based learning is also applied to information technology (IT) and security courses, although it requires full student engagement [20].

The increasing demand for privacy professionals necessitates the creation of educational programs that equip future experts with crucial skills and promote student active participation in learning [22]. Compared to traditional teaching, interactive teaching and learning tactics are now necessary to attract students' attention. Interactive learning involves active student participation and engagement during the lectures in the form of regulated dialogue [12]. This way of teaching encourages students to think about the topic and makes it more interesting for them to follow the lectures. New teaching strategies in privacy and security education started incorporating gamification elements to increase student motivation and learning experience [23-25].

Teaching privacy has become an integral part of all areas, including marketing [26], art and media workers' education [27], and human-computer interaction courses [28]. In these aspects, privacy is often explained using examples or scenarios that are familiar to students. The value of using scenario-based learning in privacy and security education is emphasized [24], [28], as it allows students to develop competencies based on real-world challenges. Interactive workshops, collaborative learning, digital resources, role-playing techniques, and guest lecturers have been considered useful strategies for educating future privacy professionals [29]. Furthermore, the closed-loop idea of "learning-doing-using" has been progressively proven to be beneficial, since it is clear that without addressing practical skills and real-world examples, it is not viable to teach dynamic subjects such as privacy protection [22].

The purpose of this research is to investigate what is students' point of view about the positive and negative aspects of the used strategies for teaching privacy-related subjects. The comprehensive content analysis method will be utilized to

address student feedback in a methodical manner and compare the results with current strategies applied in shaping future privacy education.

2. Methodology

A survey was distributed to 50 third-year undergraduate students enrolled in the Privacy and Personal Data course, examining overall satisfaction with the course lectures, laboratory exercises, project assignments, and student recommendations for improvement. In [30] we reported on how we employed the semantic differential technique to assess student satisfaction with course design and teaching strategies. Students were generally satisfied with the course design and used teaching methods. Our findings revealed that students most highly rated the 'activity evaluation of cookie policies,' deeming it useful, necessary, adequate, motivating, and conducive to learning. Conversely, 'creating project tasks' was perceived as the most challenging activity. While students found 'looking for examples of privacy breaches' most interesting, complex tasks, although considered more challenging, exhibited a slight decrease in student motivation.

This research focuses on the analysis of students' recommendations for improvement, with 31 students responding to this question. To obtain student feedback, one open-ended question was created: "We invite you to submit suggestions for improving the organization of classes in the course Privacy and personal data". The comments from each student were then converted into a text document in separate units so that they could be loaded into the content analysis tool. Content analysis was performed using free QDA Miner Lite qualitative analysis software. The initial step involved categorizing comments into positive and negative aspects of privacy teaching methods. Condensed meaning units were then extracted from the parts of the text, and codes were assigned to each of them. The codes were not predetermined, but by going through the content, some subcategories were observed, which were then classified into codes. Each of the codes was then classified into one of the superordinate categories depending on whether it was a positive or negative aspect. Further analysis and frequency calculation was carried out in the QDA Data Miner Lite qualitative analysis software.

3. Results

Contextual analysis was performed on 31 student comments gathered. Students were invited to submit their suggestions for improving the organization of lectures in the course Privacy and personal data. We identified a total of 64 condensed units of meaning and grouped them into 2 main categories named positive and negative aspects. In the positive aspects category condensed units of meaning were grouped in 6 codes, while negative aspects were separated into 8 codes. Results of contextual analysis can be seen in Figure 1., while the categories and codes will be explained in detail in the following sections.

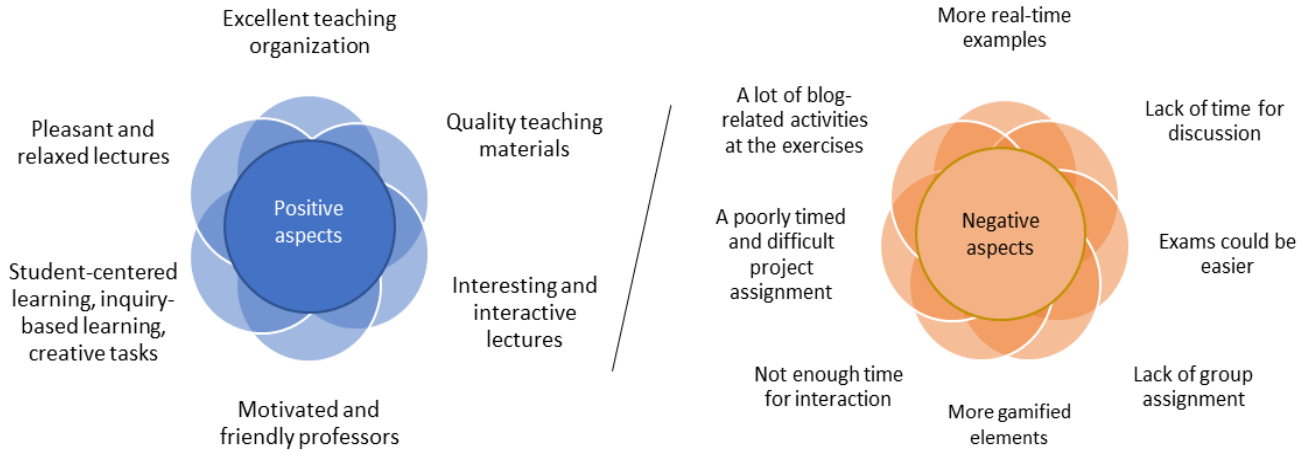

Fig. 1: Contextual analysis results

3.1. Positive aspects

The category of positive aspects included all comments in which students expressed satisfaction with utilized privacy teaching methods, as well as comments indicating that nothing needed to be changed. Table 1 shows the distribution of the 6 codes observed in the category of positive aspects.

Table 1: Distribution of codes under the category positive aspects.

Code	Meaning units of text	Count	% Codes
Excellent teaching organization	"The course is very well organized, all responsibilities are clearly defined and posted on time." "I believe that the course Privacy and Personal Data includes a wide range of different and interesting knowledge assessment concepts that are suitable for a course addressing privacy and personal data protection topics." "I found the classes to be good, especially since some lectures covered internet privacy and related areas."	24	37,50%
Quality teaching materials	"The offered project topics, additional materials for exam preparation." "…with the use of interesting methods for assessing the material, as well as engaging tools for the learned content." "…from Kahoot, the link to the online game, team tasks, the six hats method, etc."	10	15,60%
Interesting and interactive lectures	"The student is not forced to just listen, but is also involved in the discussion, which I consider extremely good." "The lectures were not long and boring, and there was plenty of interaction."	8	12,50%
Motivated and friendly professors	"The professors in this course are approachable." "…always tries to involve other students in discussions."	5	7,80%
Student-centered learning, inquiry-based learning, creative tasks	"One of the few courses that is student-oriented." "The laboratory exercises were mostly based on research, so even those who don't like studying might have remembered something by conducting research." "I like that the lessons are conducted in a creative way."	4	6,30%
Pleasant and relaxed lectures	"I learned more in this course than I expected, in a relaxed and good way." "Overall, the classes were pleasant without too much stress…"	2	3,10%

3.2. Negative aspects

The category of negative aspects included all comments in which students were not satisfied with utilized method, as well as comments indicating areas for improvement. Table 2 shows the distribution of the 8 codes observed in the category of negative aspects.

Table 2: Distribution of codes under the category negative aspects.

Code	Meaning units of text	Count	% Codes
More real-time examples	"More examples of privacy violations" "More real-world examples."	2	3,10%
Lack of time for discussion	"If possible, more time could be allocated for discussions." "Lab activities are slightly more demanding than lecture activities due to the time limit per activity."	2	3,10%
Exams could be easier	"You only need to study for the midterms..." "…simpler exams…"	2	3,10%
Lack of group assignment	"…only for easier learning maybe more group tasks to make it easier for us to learn. Personally, I remembered things more when we had a group task in the lecture that we needed to explain one thing and when we listened to our colleagues, it was easier to remember."	1	1,60%
Not enough time for interaction	"More interaction with students"	1	1,60%
A poorly timed and difficult project assignment	"Please make it a project earlier next year…"	1	1,60%
A lot of blog-related activities at the exercises	"Fewer blogs during the exercises…"	1	1,60%
More gamified elements (Kahoot, online games)	"More Kahoot and online games!"	1	1,60%

4. Discussion

Students expressed satisfaction with the course, which was designed to focus on the student as an active participant, not just a listener. The results were consistent in terms of successful teaching organization, under the code "Excellent teaching organization" (37,50%) with 24 students expressing satisfaction with the lectures that covered relevant and recent privacy topics. Under the code "Student-centered learning, inquiry-based learning, creative tasks" (6,30%) students appreciated the use of learning that refocuses the emphasis from teachers to students and fosters their research. Competition and challenge-based exercises increase students' engagement and deepen their knowledge about cybersecurity topics, 14 students reported that working in groups to solve given challenges and creating original challenges for other teams helped them learn more about the topic [10].

Under the code “Quality teaching materials” (15,60%) students emphasized that the materials created contributed to their learning and interest in the topic. It is stressed how crucial it is to produce high-quality materials so that students may study cybersecurity in an engaging and appealing way [12]. Creating materials that involves scenarios can encourage critical thinking and help students to see the issues from a different perspective [27]. Scenario-based learning in the context of cybersecurity training can improve critical thinking and problem-solving skills, such as the ability to categorize cybersecurity incidents and learn about risk mitigation [24]. According to the code "Interesting and interactive lectures" (12,50%), students valued teaching that included interaction with them. Interactive teaching and learning in security education proved to be useful for achieving the desired learning outcomes in both theoretical and practical contexts [12]. A positive learning environment is also emphasized, under the code “Motivated and friendly professors” (7,80%) and “Pleasant and relaxed lectures” (3,10%).

Students suggested that more real-world examples, as well as encouragement of discussion and collaborative effort, should be included in the teaching of these courses. In prior studies, students mentioned that real-time examples improve their understanding of cybersecurity flaws and defense strategies [10]. Giving students practical learning environments where they may carry out experiments and resolve real-world problems can be a useful tool for deepening their understanding of privacy and security concepts [11]. Under the code "Lack of group assignment" (1.60%), students emphasized the importance of working in groups to encourage their motivation and mutual learning. It was found that group discussion can be useful, especially in solving complex problems [10],

Introducing gamification can motivate students to participate, but also facilitate learning through real-world examples. For example, by participating in gamified social networks, students can learn how to responsibly manage privacy and prevent data leaks on social networks [23]. Future privacy education must incorporate game activities to help students apply their privacy knowledge to solve real-world security challenges [25].

Students expressed dissatisfaction with the project, considering it a very demanding activity. Project-based learning has proven to be beneficial when solving real-world challenges, as students feel that what they are doing is meaningful and can really help someone [20]. An opportunity to improve the course lies in collaborating with employers to address real-world challenges, aimed to encourage students to change their approach in resolving project assignments.

5. Conclusion

A student-centered approach that encourages active student participation has proven to be extremely effective. Content analysis carried out was useful for extracting categories related to their point of view on the utilized methods to teach privacy. The results showed consistency in student responses, emphasizing the importance of teaching privacy by combining different teaching methods that would engage them. Also, the inclusion of gamification elements proved useful for further stimulating student interest. Future privacy education should go in that direction, providing interactive lectures with practical examples and creative tasks. The limitations of this research refer to the relatively small number of students analyzed. Although previous research has confirmed that the application of interactive teaching that encourages students to learn has a positive effect, in order to verify the results, the application of this method should be examined on a larger number of students and potentially in different learning environments.

References

[1] Gartner, “Hype Cycle for Privacy, 2024”, 2024. Accessed: Jan. 23, 2025. [Online]. Available: https://www.gartner.com/en/documents/5622691

[2] ISACA, “State of Privacy 2025,” 2025. Accessed: Jan. 23, 2025. [Online]. Available: https://www.isaca.org/resources/reports/state-of-privacy-2025

[3] ISACA, “Privacy in Practice 2024” 2024. Accessed: Jan. 23, 2025. [Online]. Available: https://www.isaca.org/resources/reports/privacy-in-practice-2024-report

[4] ENISA, “FORESIGHT CYBERSECURITY THREATS FOR 2030-UPDATE,” 2024. Accessed: Jan. 23, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf, doi: 10.2824/349493.

[5] ISC2 Cybersecurity Workforce Study, "Global Cybersecurity Workforce Prepares for an AI-Driven World," 2024. Accessed: Jan. 23, 2025. [Online]. Available: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf
[6] ENISA, "European cybersecurity skills framework (ECSF) : user manual," 2022. Accessed: Jan. 23, 2025. [Online]. Available: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf
[7] National Institute of Standards and Technology (NIST), "NIST PRIVACY FRAMEWORK," Gaithersburg, MD, Jan. 2020. doi: 10.6028/NIST.CSWP.01162020.
[8] NIST, "NICE Workforce Framework for Cybersecurity (NICE Framework)." Accessed: Jan. 23, 2025. [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework
[9] R. Sánchez-Cabrero, J. L. Estrada-Chichón, A. Abad-Mancheño, and L. Mañoso-Pacheco, "Models on teaching effectiveness in current scientific literature," Aug. 01, 2021, *MDPI AG*. doi: 10.3390/educsci11080409.
[10] X. Wu and S. Tian, "Student-centered learning in cybersecurity in summer semester," *2015 IEEE Frontiers in Education Conference (FIE)*, pp. 1–4, 2015.
[11] M.M. Rahman, M.A. Barek, M.S. Akter, A.K. Islam Riad, M.A. Rahman, H. Shahriar, A. Rahman, F. Wu, "Authentic Learning on DevOps Security with Labware: Git Hooks To Facilitate Automated Security Static Analysis," in *2024 IEEE 48th Annual Computers, Software, and Applications Conference (COMPSAC)*, Institute of Electrical and Electronics Engineers (IEEE), Aug. 2024, pp. 2418–2423. doi: 10.1109/compsac61105.2024.00388.
[12] R. Hosler, X. Zou, and M. Bishop, "Electronic Voting Technology Inspired Interactive Teaching and Learning Pedagogy and Curriculum Development for Cybersecurity Education," in *IFIP Advances in Information and Communication Technology*, Springer Science and Business Media Deutschland GmbH, 2021, pp. 27–43. doi: 10.1007/978-3-030-80865-5_3.
[13] J. Yang, Y. Rae Kim, and B. Earwood, "A Study of Effectiveness and Problem Solving on Security Concepts with Model-Eliciting Activities," in *Proceedings - Frontiers in Education Conference, FIE*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/FIE56618.2022.9962412.
[14] G. Nuthall, "Relating classroom teaching to student learning: A critical analysis of why research has failed to bridge the theory-practice gap," *Harvard educational review* , vol. 74, no. 3, pp. 273–306, 2004.
[15] I. Dionysiou and D. Ktoridou, "Enhancing Dynamic-Content Courses with Student-Oriented Learning Strategies," *International Journal of Cyber Ethics in Education*, vol. 2, no. 2, pp. 24–33, Apr. 2012, doi: 10.4018/ijcee.2012040103.
[16] X. Yuan, T. Zhang, A.A. Shama, J. Xu, L. Yang, J. Ellis, W. He, C. Waters, "Teaching cybersecurity using guided inquiry collaborative learning," *2019 IEEE Frontiers in Education Conference (FIE)*, pp. 1–6, 2019.
[17] J. von Hoyer, A. Hoppe, Y. Kammerer, C. Otto, G. Pardi, M. Rokicki, R. Yu, S. Dietze, R. Ewerth, P. Holtz, "The Search as Learning Spaceship: Toward a Comprehensive Model of Psychological and Technological Facets of Search as Learning," Mar. 15, 2022, *Frontiers Media S.A.* doi: 10.3389/fpsyg.2022.827748.
[18] A. De, M.N.I. Khan, K. Nagarajan, A.A. Saki, M. Alam, T. Wood, M. Johnson, M. Saripalli, Y. Xia, S. Cutler, S. Ghosh, K. Hill, A. Ward, "Hands-On Cybersecurity Curriculum using a Modular Training Kit," in *ASEE Annual Conference and Exposition, Conference Proceedings*, 2020.
[19] J. R. Savery, "Overview of Problem-based Learning: Definitions and Distinctions," *Interdisciplinary Journal of Problem-Based Learning*, vol. 1, no. 1, May 2006, doi: 10.7771/1541-5015.1002.
[20] L. Simpkins, X. Yuan, J. Modi, J. Zhan, and L. Yang, "A course module on web tracking and privacy," in *Proceedings of the 2015 Information Security Curriculum Development Conference, InfoSec CD 2015*, Association for Computing Machinery, Inc, Oct. 2015. doi: 10.1145/2885990.2886000.
[21] D. Pheils, "Applying a community project approach to IT and security courses," in *Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference*, ACM, 2013, pp. 79–87.
[22] S. Zhe, N. Hong, Y. Lihua, and F. Binxing, "A preliminary study on the construction of _Data Privacy Protection_ course based on teaching and training range," *Journal of Network & Information Security*, vol. 9, no. 1, 2023, Accessed: Jan. 11, 2025. [Online]. Available: https://www.infocomm-journal.com/cjnis/article/2023/2096-109X/2096-109X-9-1-00178.shtml

[23] J. Alemany, E. Del Val, and A. Garcia-Fornes, "Assessing the Effectiveness of a Gamified Social Network for Applying Privacy Concepts: An Empirical Study with Teens," *IEEE Transactions on Learning Technologies*, vol. 13, no. 4, pp. 777–789, Oct. 2020, doi: 10.1109/TLT.2020.3026584.

[24] R. Pirta-Dreimane, A. Brilingaitė, E. Roponena, K. Parish, J. Grabis, R.G. Lugo, M. Bonders, "Try to esCAPE from Cybersecurity Incidents! A Technology-Enhanced Educational Approach," *Technology, Knowledge and Learning*, 2024, doi: 10.1007/s10758-024-09769-8.

[25] W. Vigl and S. Abramova, "Design and Use of Privacy Capture-the-Flag Challenges in an Introductory Class on Information Privacy and Security," in *Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE*, Association for Computing Machinery, Jul. 2024, pp. 618–624. doi: 10.1145/3649217.3653572.

[26] J. W. Peltier, G. R. Milne, J. E. Phelps, and J. T. Barrett, "Teaching information privacy in marketing courses: Key educational issues for principles of marketing and elective marketing courses," *Journal of Marketing Education*, vol. 32, no. 2, pp. 224–246, Aug. 2010, doi: 10.1177/0273475309360164.

[27] Y. W. Lin, "A reflective commentary of teaching critical thinking of privacy and surveillance in UK higher education," Jun. 01, 2017, *SAGE Publications Ltd*. doi: 10.1177/2053951717694054.

[28] S. Ovaska and K.-J. Räihä, "Teaching Privacy with Ubicomp Scenariosin HCI ClassesOpen 247," in *Proceedings of the 21st Australasian Computer-Human Interaction Conference*, ACM Digital Library, 2009, pp. 105–112.

[29] A. Sharma, "Teaching Digital Privacy: Navigating the Intersection of Technology, Education, and Privacy", [Online]. Available: www.kanpurhistorians.org

[30] R. Mekovec and M. Kuštelega, "HOW TO TEACH PRIVACY: ASSESSMENT OF INNOVATIVE LEARNING APPROACHES FOR UNDERGRADUATE STUDENTS.", in *Proceedings of the 21st International Conference on Cognition and Exploratory Learning in the Digital Age (CELDA 2024)*, 2024, pp. 217-224.