USAGE OF PRIVATE DATA FROM ONLINE PLATFORMS BY GOVERNMENTS AND COMPANIES: STUDY OF STUDENTS' AWARENESS AND CONCERNS

Sanja Adjaip-Velichkovski
International Balkan University, Skopje, N. Macedonia, s.adzaip@ibu.edu.mk

Abstract: In this digital era individuals access information and communicate in new ways, changing how everyone conducts business. Today, social media, e-commerce platforms, search engines, and cloud services provide effortless engagement and connectivity, making it easier to stay digital. This increased reliance on digital platforms raises concerns about how governments and private corporations collect, store, and utilize personal data. Increased use of artificial intelligence (AI), availability of big data, and automated decision-making are not only making it easier for organizations to monitor, process, and use customer-related information for enhancing services and improving user experience and infrastructure, but also is raising questions of privacy and data protection.
Utilizing both theoretical and empirical perspectives, this study employs a quantitative research approach to assess students' concerns about data privacy. A structured questionnaire, adapted from UNESCO (2017) and consisting of 24 multiple-choice questions, was used to collect data from IBU students. The survey, conducted in April 2024, was administered online, allowing respondents to participate anonymously via computers, tablets, or smartphones. This paper presents the results from the third part of the larger research, focusing on answering the question of students' perspectives on the use of private data from online platforms by governments and companies. Other research questions addressed in this survey explore the significance of online privacy and safety (Adjaip-Velichkovski, S. 2024), students' perspectives on the importance of privacy and safety knowledge in the digital age (Adjaip-Velichkovski, S., Dzigal, S. 2024), and the importance of protection of others' privacy on digital platforms.
Keywords: private data, online platforms, governments, companies, privacy

1. INTRODUCTION

The contemporary digital landscape is characterized by the torrent of collection of historically unprecedented data, especially in the context of individual data collected by corporations and states. With progress in technology, means through which data are harvested and processed have grown to include multiple platforms, the privacy and data of which have significant consequences for security. Institutions tend to gather students' information for improving learning outcomes, resource management, and services; Nonetheless, the extent of this gathering and the kind amplify privacy issues for the students. Current research has revealed a growing public distrust of how the numbers are being utilized, especially in environments where the data might be transferred or sold to third parties, typically in an uninformed fashion (Wills, 2024). Such fear has been added to by revelations of high-level data breaks and government spying methods, increasing the need for rigid regulatory systems to protect personal privacy rights.
On this point, the purpose of this paper is to look at how students react towards the practices of the governments and corporations in using their own information. By discussing the attitude and perception of the students toward the privacy of the information, we seek to highlight the underlying problems that drive their fear. Particularly, we discuss the results of the survey outlining the perception of students regarding multiple aspects of the data collection procedure, including the alleged advantages, risks, and ethical considerations in the application of private information. These answers will be presented in visual format with graphics that attempt to emphasize the central issues arising from the data, which is a testament to students' good understanding of the intersection of technology, privacy, and regulatory control. With this discussion, this paper attempts to make contributions to existing debates on information privacy in the education sector and alerts political powers and schools to the need for effective regulations and compulsion for guidelines that place great emphasis on students' right to privacy. The research work done in this paper is intended to examine the students' approaches towards use of private information. A mixed methods approach was followed combining the quantitative and qualitative data collection methods; the participants' awareness and approach (Almahesses et al., 2021; Chitus et al., 2023) are needed to attain independent insight into.

2. DATA COLLECTION CONCERNS

The growing dependence on online platforms for social interaction, commerce, and information has led to a generalized collection and use of private data by governments and corporations. This phenomenon raises significant ethical implications regarding privacy, security, and consent of users. As the policy formulators deal with the ambiguities of this new digital panorama, several socio-legal, technological, and political perspectives arise that can illuminate the ethical tensions inherent in personal data management.

The act of collecting and using data can often blur the lines between beneficial and exploitative practices. Governments and corporations justify their use of data through national security lenses, the improvement of economic service, and growth. However, as Chatterjee and NS (2023) suggest, this data exchange manifests a network of paradoxes where the expected benefits can contravene the expectations of privacy and autonomy of users. Ethical considerations must expand beyond the mere fulfillment of legal frameworks to cover a deeper understanding of the user's consent.

The user's consent is frequently represented as a binary choice between agreement and rejection; However, reality is much more complex. Many users still do not realize the wide range of data collected and the implications of their consent (Beverungen et al., 2022). This ignorance highlights a fundamental ethical concern: are the users who really provide informed consent, or are they coerced into acceptance under the appearance of convenience? The concept of "consent fatigue", as illustrated by Quach et al. (2022), represents a landscape where users continuously agree on the terms of service without integrally understanding them, perpetuating the uninformed consent cycle.

In addition, the growing power of online platforms raises critical questions about the morality of using personal data for profit. Corporations often argue that data collection is a means of optimizing and improving user experiences. However, as Akman (2021) states, empirical evidence suggests that users are unclear and sometimes hostile to commercialization of their personal data. This ambition indicates increasing dissatisfaction with compensation between convenience and privacy, reducing the alleged moral standards of consent. In collaboration with corporate interests, the government's access to private data presents additional moral implications, especially in relation to national security. Monitoring capabilities provided by data aggregation can lead to an intrusion, potentially eradicate civil freedom (Cramers, 2022). Critics argue that such practices can promote an atmosphere of fear and mistrust, refuting democratic values that many governments prepare to defend. As Cioffi et al. (2022) argue that governments require re-evaluation of regulatory framework to mimic corporate data practices that control the use of data. To ensure better transparency and responsibility measures, there is an immediate requirement to prioritize moral ideas on public and private sector profits and control. Ethical implications around the use of data also reach security concerns. Violations or misuse of personal data can cause serious consequences, including identity theft and loss of financial assets (Flave, 2021). The bets are particularly high for the weaker population that may lead to a lack of resources to overcome such incidents. The need for solid safety protocols cannot be exaggerated, highlighting a moral obligation for corporations and states to strictly secure user data. Additionally, Gawer and Srnicek (2021) affirm that the social repercussions of failed data security measures can have long -range implications, possibly undermine confidence in digital ecosystems and force users out of line.

In response to these challenges, the presence of regulatory framework for the purpose of combating small moral data has achieved impulses. The concept of self-regulation, as presented by Kasumano et al. (2021), proposes that digital platforms voluntarily adopt moral standards, possibly prevailing the need for more strict legal supervision. However, the effectiveness of such self-regulating mechanisms remains debatable. Without empirical evidence that demonstrates its success or the political will to enforce compliance, self-regulation seems to function more as an aspirational ideal than as a tangible solution to the ethical dilemmas raised by the use of data.

In addition, legislative approaches vary between courts, which leads to a fragmented global panorama about data security. Such inequalities are pronounced in terms of implications and rich digital ecosystems, which require real-time data processing and exchange (Bibri et al., 2022). While innovative technologies promise to improve the user experiences, they also complicate the moral discourse that surrounds privacy and data security, as the principles that control online interactions give more rest in the name of progress. Ultimately, moral implications of governments and corporations that use private online platform data emphasize a versatile examination of users' privacy, security and consent. Achieving a balanced approach that respects individual rights while promoting innovation and safety requires continuous communication and adjustment in the regulatory landscape. To pay attention to this balance, cultivation of a resistant digital ecosystem requires continuous participation of interested parties, including users, governments and corporate institutions. As technology develops, our moral outlines should also address the complications of data usage in a world that changes rapidly.

3. METHODOLOGY

The purpose of this study is to look at students' knowledge and concerns within the International Balkan University of online security and privacy, specifically with reference to governments and companies. To address this aim, a quantitative research approach was employed. A standardized questionnaire was employed to collect data on the awareness level of the students in terms of privacy and online safety concerns. The survey contained items that assessed personal experience with demographic information, perceptions of government and business, knowledge about online privacy policies and invasion, subjective concern and perception based on Likert scale items in order to statistically analyze responses. Data collection was organized for completeness and availability within an internet-

based survey format enabling honest responses regarding sensitive issues. In April 2024, an online survey was conducted with a questionnaire sent to students at the International Balkan University in Skopje, North Macedonia. The questionnaire was accessible on a variety of devices like computers, tablets, and smartphones to make more respondents participate. The response was purely voluntary, and confidentiality was assured since personally identifiable information was not requested. Additionally, as the survey was conducted online and without the presence of the interviewer, the potential for bias was minimized. The results of this research will provide valuable information about the awareness and concerns of the student population at the International University of Balkan towards the use of private information from online sources by governments and all types of companies and will contribute to a massive debate on data security.

4. USAGE OF PRIVATE DATA FROM ONLINE PLATFORMS BY GOVERNMENTS AND DIFFERENT TYPES OF COMPANIES

In the contemporary digital scenario, the use of private data by governments and corporations has emerged as a relevant question. Private data includes a wide range of information, including individual identifiers, consumer behavior, and digital footprints, which is rapidly used for various purposes such as marketing, monitoring, and public policy making. Private data use means not only in its ability to improve services and governance efficiency, but also in the ability to increase the violation of important moral concerns and privacy. As Gawer and Srnicek (2021) note, it is necessary to understand the complex interaction between data, governance, and social values to address the duality of its benefits and risks. For the purposes of this research, a web-based survey was randomly distributed to students, allowing participants the flexibility to complete it at their convenience. As previously stated, the target population comprises students from the International Balkan University in Skopje, North Macedonia. Participants were asked to provide demographic information, including gender and age, the results of which are summarized below. A total of 145 responses were collected, forming a representative sample of the university's student body. As shown in Table 1, the sample includes 103 female participants, 41 male participants, and one nonbinary respondent. The age of participants ranged from 18 to 27 years.

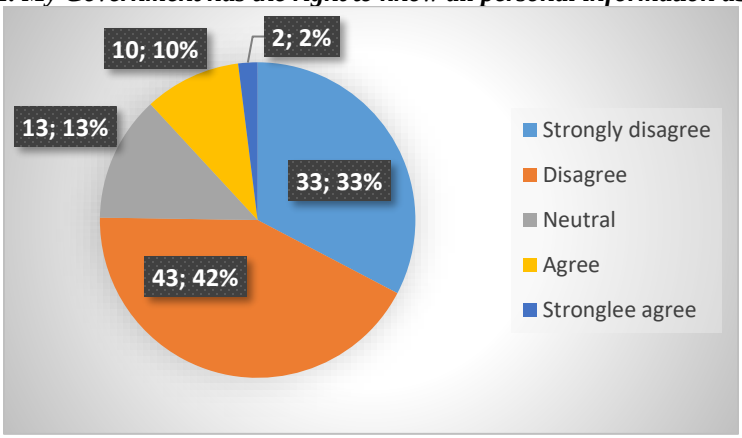
Table 1. Total number of participants

Total number of participants	Male	Female	Nonbinary
145	103	41	1

Source: Results from own work

The survey results presented in Figures 1 through 6 offer valuable insights into students' attitudes toward data privacy, surveillance, and institutional control over personal information in online environments.

Figure 1. My Government has the right to know all personal information about me.

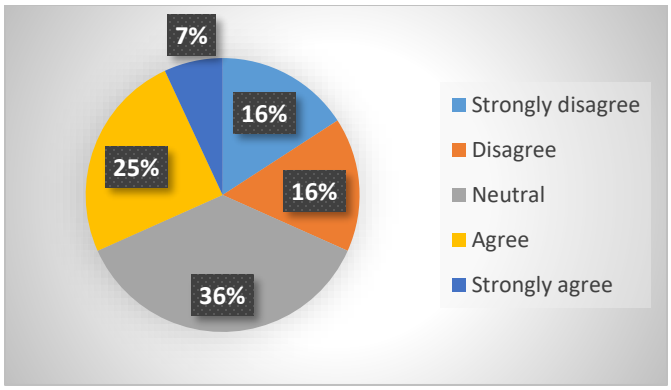


Source: Results from own work

The data gathered indicate that a significant number of students at International Balkan University express skepticism regarding the government's right to access personal information. Although a minority of respondents agree or strongly agree with such access, the overall sentiment leans toward disapproval. This suggests a fundamental concern among students regarding governmental overreach into personal privacy. As illustrated in Figure 1, the majority of respondents either disagreed or strongly disagreed, indicating a general reluctance to accept

unrestricted governmental access to personal data. This finding underscores the persistence of privacy concerns among youth, even in the context of state institutions that may claim legitimacy or public interest in their data collection practices.

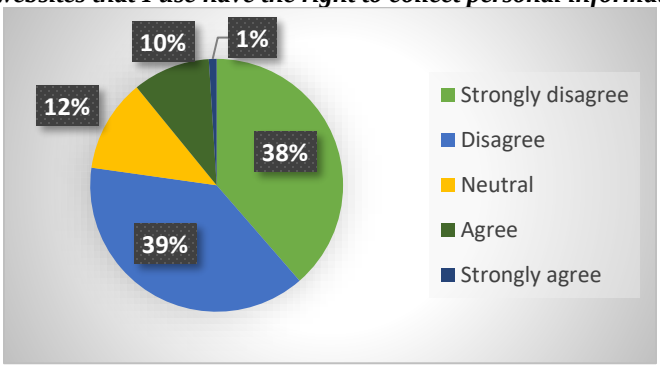
Figure 2. My government has the right to know all personal information about me if this will keep me safe online.



Source: Results from own work

When the condition of online safety is introduced, responses shift slightly, showing a moderate increase in agreement with government data access. The results in Figure 2 explore a more conditional question—whether such access would be acceptable if it enhances online safety. Here, a slight increase in agreement is observed, with a notable proportion of respondents selecting a neutral stance. This indicates a degree of pragmatic reasoning among some students, who may be willing to compromise privacy for enhanced security. However, the high level of neutrality also suggests uncertainty or ambivalence regarding the trade-off between personal privacy and public safety.

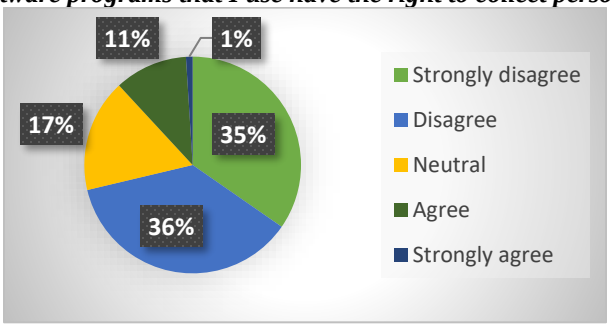
Figure 3. All websites that I use have the right to collect personal information about me.



Source: Results from own work

The participants exhibit notably higher resistance to the idea of websites collecting personal data, as illustrated in Figure 3. An overwhelming majority disagreed or strongly disagreed with the proposition, indicating a pronounced distrust of commercial entities managing personal information. This trend is consistent when applied to computer software programs as well, where students again express a strong reluctance to permit such data collection. These results imply that students perceive corporate data practices as more intrusive or less justified than those undertaken by governments, even under the premise of public safety. This suggests that students differentiate between state and corporate data practices, viewing the latter as more intrusive or profit-driven.

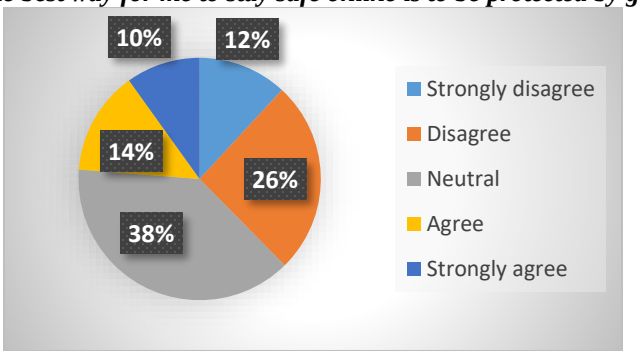
Figure 4. All computer software programs that I use have the right to collect personal information about me.



Source: Results from own work

As illustrated in Figure 4, which presents responses to a similar question regarding software programs, the pattern of responses closely mirrors that of Figure 3, reinforcing the finding that students harbor significant reservations toward data collection by private companies. This consistency highlights a generalized distrust in commercial digital platforms and applications when it comes to handling personal information.

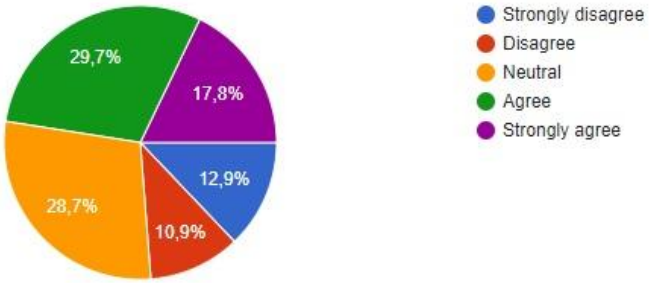
Figure 5. The best way for me to stay safe online is to be protected by government.



Source: Results from own work

Regarding the perception of safety online, student opinions are more divided. While a notable portion disagrees with the notion that government protection is the best means to ensure online safety, a large number of students also have a neutral position. This diversity in responses reflects the ongoing ambivalence or complexity in attitudes toward the appropriate role of government in digital security. The results in Figure 5 examine the perceptions of government responsibilities in ensuring online security. The reactions were particularly diverse, with a sufficient number of students expressing disagreements, and a significant part of the students selecting a neutral reaction. This polarization suggests that when some students consider government intervention as beneficial for digital safety, others are careful with increased state control or monitoring under the guise of security.

Figure 6. The internet should be an open space free from control by government or big businesses



Source: Results from own work

Finally, the internet-related statement received various reactions as a place free from government or corporate control of the Internet. Although a part of the students supported the idea, many either disagreed or chose a neutral stance. This may suggest awareness about the fine challenges associated with maintaining an open internet, especially in the context of misinformation, cyber threats, and regulatory rules. Finally, Figure 6 evaluates support for an open internet free from government or corporate control. The reactions were mixed, with significant disagreement and neutrality. These results point to the complexity of the student's approach; While many advocate digital independence, others recognize the potential risks associated with a perfectly irregular digital location.

5. CONCLUSION

The study highlights the need to integrate students' voices in future policy discussions, which is an essential step towards detailed rules that not only protect privacy rights but also align with moral standards expected by the student population. It is necessary that interested parties, including teachers and policymakers, identify that students' ideas are important in shaping the integral understanding of privacy problems. The findings highlight a complex and layered perspective among students about privacy, security, and digital rules. While there is clear resistance to private data collection by companies, the role of the government is seen with cautious ambition, especially when implicated in terms of security. Data suggests that while students strongly oppose corporate monitoring, their views on government access and regulation are more substantial. The high incidence of neutral reactions in many questions means that further education on data rights, digital safety, and institutional responsibilities may be necessary to support informed opinions on these important issues. In addition, this analysis of the results shows a need for further research in order to detect dynamic methods to improve data in the government and improve responsibility. It is an opportunity to check how educational institutions can apply the response system that guarantees the participation of students in decision-making processes about data use. Any future research should also focus on longitudinal studies to evaluate how students' perceptions develop in response to changing policies and technological progress. In summary, the results from the synthesis indicate that there is an important requirement for a regulatory framework that prefers transparency. The implications of this study are significant, advocating for collaboration efforts that prioritize protecting students' privacy while adopting the potential benefits that data-based approaches can offer in the field of education. As we advance, emphasizing the participation of students in these discussions will be vital for the establishment of a fairer, informed, and privacy educational landscape.

REFERENCES

Adjaip-Velichkovski S. (2024) Privacy and safety online: Students perspective, KNOWLEDGE - International Journal. https://ikm.mk/ojs/index.php/kij/article/view/6902

Adjaip-Velichkovski, S., & Dzigal, S. (2024) The critical role of privacy and safety knowledge in the digital age, KNOWLEDGE- International journal. https://ikm.mk/ojs/index.php/kij/article/view/7290

Akman, P. (2021). A web of paradoxes: empirical evidence on online platform users and implications for competition and regulation in digital markets. Va. L. & Bus. Rev., 16, 217. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/valbr16§ion=11

Almahasees, Z., Mohsen, K., & Amin, M. O. (2021, May). Faculty's and students' perceptions of online learning during COVID-19. In Frontiers in education (Vol. 6, p. 638470). Frontiers Media SA.

Beverungen, D., Hess, T., Köster, A., & Lehrer, C. (2022). From private digital platforms to public data spaces: implications for the digital transformation. Electronic Markets, 32(2), 493-501. https://link.springer.com/article/10.1007/s12525-022-00553-z

Bibri, S. E., Allam, Z., & Krogstie, J. (2022). The Metaverse as a virtual form of data-driven smart urbanism: platformization and its underlying processes, institutional dimensions, and disruptive impacts. Computational Urban Science, 2(1), 24. https://link.springer.com/article/10.1007/s43762-022-00051-0

Chatterjee, S., & NS, S. (2023). Impact of AI regulation and governance on online personal data sharing: from sociolegal, technology and policy perspective. Journal of Science and Technology Policy Management, 14(1), 157-180. https://www.emerald.com/insight/content/doi/10.1108/JSTPM-07-2020-0103/full/html

Chytas, K., Tsolakidis, A., Triperina, E., Karanikolas, N. N., & Skourlas, C. (2023). Academic data derived from a university e-government analytic platform: An educational data mining approach. Data in Brief, 49, 109357.

Cioffi, J. W., Kenney, M. F., & Zysman, J. (2022). Platform power and regulatory politics: Polanyi for the twenty-first century. New Political Economy, 27(5), 820-836. https://www.tandfonline.com/doi/abs/10.1080/13563467.2022.2027355

Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011. https://academic.oup.com/cybersecurity/article-pdf/doi/10.1093/cybsec/tyac011/47918796/tyac011.pdf

Cusumano, M. A., Gawer, A., & Yoffie, D. B. (2021). Can self-regulation save digital platforms?. Industrial and Corporate Change, 30(5), 1259-1285. https://academic.oup.com/icc/article-abstract/30/5/1259/6355574

Flew, T. (2021). Regulating platforms. John Wiley & Sons. https://books.google.com/books?hl=en&lr=&id=fI1SEAAAQBAJ&oi=fnd&pg=PA1986&dq=Private+data+usage+by+governments+and+companies+on+online+platforms:+implications+and+regulations&ots=9IVOLvpmyb&sig=soHFk0WxfmV61lDtyPmI8IpW5Ik

Gawer, A., & Srnicek, N. (2021). Online platforms: Economic and societal effects. https://kclpure.kcl.ac.uk/portal/files/149143202/EPRS_STU_2021_656336_EN.pdf

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323. https://link.springer.com/article/10.1007/s11747-022-00845-y

Willse, C. (2024). State education agency governance, virtual learning, and student privacy: Lessons from the COVID-19 pandemic. Educational Policy, 38(1), 186-217.