Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Trinity University, Lagos, Nigeria
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
Harmarth Global Educational Services
ICT University Foundations USA
IEEE Computer Society Nigeria Chapter

Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference

Right to Privacy on The Internet

Boateng Christiana
Information Technology and Law Graduate Programme
Ghana Institute of Management and Public Administration
Greenhill, Accra, Ghana
Email: christiana.boateng@st.gimpa.edu.gh
Phone: +233554663502

ABSTRACT

This study aims on Right to Privacy on the Internet. The paper will unfold as follows. Influences on consumer privacy online, online consumer tracking; that is when online scenarios meet privacy expectations or complied with a privacy notice, and the importance of privacy notices in managing privacy online. This paper will also highlight consumer online privacy specifying ''the youth, parents, and online privacy' 'and the regulations in place to shape such policies. Will also unfold privacy in the digital age or the internet. This paper will again unfold UN general assembly on the right to privacy on the internet. The paper unfolds the potential consequences of revealing certain information online and analyzes if there are any differences between the motivations and attitudes of young people. Will again highlight on National Security Agency (NSA) surveillance which demands that Internet carriers be more forthcoming about their handling of personal information which must be intensified. Responding to this concern, this report evaluates the data privacy transparency of forty-three Internet carriers serving the public. This paper is to investigate the relationship between individual and societal determinants of online privacy concern (OPC) and behavioral intention of internet users. The study also aims to assess the degree of reciprocity between consumers' perceived benefits of using the internet and their OPC in the context of their decision-making process in the online environment.

Keywords: Internet, Privacy, Internet Privacy Right, Internet Privacy, Online Privacy, Digital Age.

Proceedings Citation Format
Boateng Christiana (2023): Right to Privacy on The Internet. Proceedings of the 36th iSTEAMS Accra Bespoke Multidisciplinary Innovations Conference. University of Ghana/Academic City University College, Accra, Ghana. 31st May – 2nd June, 2023. Pp 165-174. https://www.isteams.net/ghanabespoke2023. dx.doi.org/10.22624/AIMS/ACCRABESPOKE2023P16

1. BACKGROUND TO THE STUDY

1.1. What is Internet Privacy?

It is the ability of internet users to control the flow of information and have reasonable access to data generated during a browsing session. This entrusts enormous quantities of personal data produced by our online activities to a select group of Internet carriers. These carriers, also referred to as Internet service providers (ISPs) or telecommunication service providers (TSPs), carry, transmit, and route data back and forth over the Internet between personal devices (laptops, smartphones, etc.), e-mail servers, websites, social networking sites & other services.

The personal information carried in these messages, as well as the associated metadata, is often sensitive and highly revealing of our private lives, of our desires, affiliations, movements, social networks, spending habits, and so forth. It is not surprising, then, that as the as the population of every country expands, so too does a range of privacy concerns about Internet carriers surveilling and monitoring our personal information. Beyond the commercial uses and abuses of this potentially sensitive information, the recent revelations of US National Security Agency (NSA) whistle-blower Edward Snowden validate longstanding privacy concerns. The evidence strongly indicates that it is not just businesses analysing the details of our online activities, but that state signals intelligence agencies, such as the NSA and Communications Security Establishment (CSE), have secretly gained the cooperation of Internet carriers to capture, without prior suspicion, our data as it flows across their networks.

1.2. Three illustrative privacy issues online

i. Through 'Sponsored Stories,' Facebook users who clicked on 'like' buttons had pictures of themselves with an endorsement sent to their friends in a what looked like sponsored advertising (Kravets 2012).

ii. The travel site Orbitz tracks how users arrived at their site to prioritize search results: if a user arrived at Orbitz from a competitor's site, Orbitz may prioritize results based on price (Mattioli 2012). Similarly, Facebook mines users' browser history to target advertising.

iii. Verizon offers a service-Precision Market In sights-to business customers to mine Verizon's customer call and web browsing information to map where people are located and the types of services they purchase and use (Hill 2012). In an aptly titled article: "Verizon Very Excited That It Can Track Everything Phone Users Do and Sell That to Whomever Is Interested," Kashmir Hill outlines the service Verizon offers to businesses to track their potential customers: "we [Verizon] understand what our customers' daily activity stream is...," and Verizon sells that activity stream to their commercial customers.

1.3. Privacy Management Strategies

Privacy measurement strategies consist of

i. privacy disclosure
ii. privacy boundary linkage, and
iii. privacy boundary control.

Privacy disclosure These were adapted from measurement items used in earlier research based on the three-dimensional approach (Chen, 2018; Child et al., 2009) and it is indicated as; privacy boundary linkage: $\beta = -0.17$, $SE = 0.03$, $p < 0.01$; privacy boundary control: $\beta = 0.15$, SE 5 0.03, $p < 0.01$). These are interaction patterns which indicate the negative association between perceived privacy risk and information disclosure. This occurs only among teens who receive a high level of active mediation (M +1SD). There is a weaker association among teens who receive a lower level of active mediation (Medium: M and Low: M-1SD).

Privacy boundary linkage.

Privacy boundary linkage measures the extent to which users connected with other users and expanded their collective privacy boundaries.

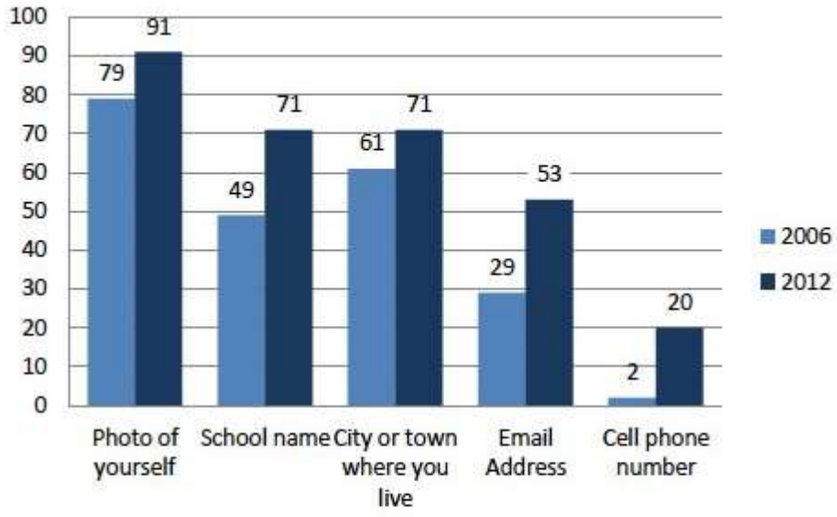
Privacy boundary control

Lastly, privacy boundary control assessed the degree to which users actively managed privacy boundaries by monitoring and controlling the personal information shared among teens. The items were carefully reviewed by TikTok users. The questionnaire items were then refined based on their feedback. The questionnaire was in Simplified in English and Spanish, the official written language of Spain.

Privacy disclosure was measured by assessing users' agreement with six items, including "I like to share my personal feelings on teens and "I like to share details about my life with teens."

Privacy boundary linkage was assessed by asking how often users engaged in activities such as "making videos using other people's videos (e.g., duet or reaction videos)" and "allowing other people to cite your videos in their videos".

Finally, **privacy boundary control** was measured by asking respondents to rate the frequency of their engagement in activities such as "asking someone to untag you from a post" or "deleting something you posted".



Source: Pew Internet Parent/Teen Privacy Survey, July 26-September 30, 2012. n=802 teens ages 12-17. Interviews were conducted in English and Spanish and on landline and cell phones. Margin of error for results based on teen social media users is +/- 5.1 percentage points. Comparison data for 2006 comes from the Pew Internet Parents & Teens Survey, October 23-November 19, 2006. n=487 teens with a profile online. Margin of error is +/- 5.2 percentage points.

Fig 1: Social Media Profiles

1.4. Implementation of All Five Fair Information Practice Principles to increase online commerce.

i. **Notice:** Online consumers should be given notice of an entity's information practices.
ii. **Choice:** Consumers should be given choice with respect to the use and dissemination of information collected from or about them.
iii. **Access:** Consumers should be given access to information about them collected and stored by an entity.
iv. **Security:** Data collectors should take appropriate steps to ensure the security and integrity of information collected.
v. **Redress:** Enforcement mechanisms, through self-regulation, government regulation, or other means, should be available to ensure compliance.

Fig 2: Fair Information Practices

Table 1: The Fair Information Practices

Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

Source: Organization for Economic Cooperation and Development.

The Federation of Trade Commission is in the process of identifying ways to assess the efforts of both the online industry and individual marketers to address privacy concerns. What is absent from the FTC's consideration, however, is the voice of online consumers about their attitudes and opinions regarding privacy concerns. The only consumer voice heard to date in FTC testimony has been using broad-based consumer telephone polls (e.g., BusinessWeek 1998; Equifax- Harris 1996), which assess privacy concern primarily through a single generic question: **How concerned are you about privacy online?** This single question cannot effectively assess privacy concern, primarily because of the "complex array of individual consumer attitudes about privacy" (FTC 1996, p. 2) and the variety of online marketing activities that may evoke varying levels of concern. Consumers' decisions to divulge personal information vary with both the individual and the context (Cranor, Reagle and Ackerman 1999; FTC 1996). Ultemately, success as a marketing communication e-commerce hinge on consumer acceptance on this medium.

1.5. UN General Assembly on Right to Privacy on the internet

Research have found that users of the internet have expectations around the type of information accessed and how it is used, using mobile app. apps (Shilton and Martin 2013) and online (Martin 2014)

This has led to UN general assembly resolution on the right to privacy on the internet which reaffirms the following:

i. The right to privacy, according to which no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, and the right to the protection of the law against such interference, as set out in article 12 of the Universal Declaration of Human Right and article 17 of the International Covenant on Civil and Political Rights.
ii. Recognizes the global and open nature of the Internet and the rapid advancement in information and communications technologies as a driving force in accelerating progress towards development in its various forms.
iii. Affirms that the same rights that people have offline must also be protected online, including the right to privacy.
iv. Calls upon all States:
    (a) To respect and protect the right to privacy, including in the context of digital communication.
    (b) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law
    (c) To review their procedures, practices, and legislation regarding the surveillance of communications, their interception, and the collection of personal data, including mass surveillance, interception, and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.
    (d) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception, and the collection of personal data.
v. Requests the United Nations High Commissioner for Human Rights to submit a report on the protection and promotion of the right to privacy in the context of domestic and extraterritorial surveillance and/or the interception of digital communications and the collection of personal data, including on a mass scale, to the Human Rights Council at its twenty-seventh session and to the General Assembly at its sixty-ninth session, with views and recommendations, to be considered by Member States.
vi. Decides to examine the question at its sixty-ninth session, under the sub-item entitled “Human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms” of the item entitled “Promotion and protection of human rights”.

1.6. Purpose of this paper

The purpose of this paper is to have understanding on what internet privacy is, the concerns of internet user about online privacy issues, implementation of privacy management strategies, examine the extent to which our knowledge of privacy concern in traditional direct marketing applies in the online context and to assess the current FTC's policies in the light of such concerns. FTC policies considering such concerns. Specifically, this study reports the results of an e-mail survey administered to a national probability sample of 889 online users. We investigate influences on consumer privacy online that have been identified by several sources, including the FTC and the current body of literature on privacy and the Internet, and analyse these influences to assess the underlying factors of privacy concern online. We discuss these findings considering the FTC's findings on privacy concerns and provide implications for public policy, Internet marketers, and further research on how UN general assembly resolution has catered for privacy on the use of internet.

1.7 Research Methodology

Only book chapters and peer-reviewed journal articles are included in this work because they contain the core arguments raised in working papers and conference proceedings. Articles used were downloaded from Emerald Full Text, Ebscohost, and JSTOR. The search descriptors used for the above stated databases were internet privacy, online privacy. The articles used were those published between 2018 and 2023. The discussions under the conceptual approaches of the respective authors were merged into a comprehensive piece.

2. RELATED LITERATURE

We proceed to explore literature contents in this section

i. **Youth and online privacy:** This study aims to explore the main concerns and attitudes adolescents have regarding online privacy. It analyses their motivations for sharing private information and the kind of information they share. Likewise, it examines whether they consider the potential consequences of revealing certain information online and analyses if there are any differences between the motivations and attitudes of young people.

ii. **How complying with a privacy notice is related to meeting privacy expectations**: Online privacy persists as a public policy issue because consumers remain concerned about online behavioural advertising and related tracking (Leon et al. 2013; McDonald and Cranor 2008; Ur et al. 2012)
In other words, many Internets users dislike being tracked, and people care about the scope and sharing of even innocuous information (Leon et al. 2014). Fair Information Practice Principles (FIPPs) have been the primary tools within public policy and practice to address privacy expectations online.

iii. **Prioritizing Privacy: A Constitutional Response to the Internet:** Beginning with the well-established notion that the Internet threatens informational privacy, this Article takes several uncharted steps toward the conclusions that the Internet calls for a constitutional right to
informational privacy and that, that right should first be sought in the state constitutions. informational privacy is discussed as more strongly concerned with the use and dissemination of personal information.

3. FINDINGS

i. The study found that online users' privacy awareness, privacy experience, personality and cultural differences significantly and positively impact their privacy concerns, which in turn positively and significantly influence their online information disclosure.

ii. The study again found that Federation of Trade Commissions policy program provides guidelines for internet users and marketers.

iii. The findings show that computer anxiety and perceived quality of regulatory framework are significant antecedents of online privacy concern (OPC), while traditional values and inclinations toward security, family, and social order; and social trust are not.

iv. Furthermore, the study reveals that perceived benefits of using the internet are the predominant factor explaining the intention to share personal information and adopt new technologies, while OPC dominates in explanation of protective behaviour.

v. The study conducted found that the Internet accelerates the trend toward increased information collection and facilitates unprecedented flows of personal information. Cellular telephones and other wireless communication technologies generate information about an individual's location and movements in a manner not possible until now. Electronic com- munication systems generate vast quantities of transactional data that can be readily collected and analysed. And law enforcement agencies, particularly at the federal level, place increasing emphasis on electronic surveillance. Confronted by these challenges, there are still grounds for optimism.

vi. The paper also recalls dangers to privacy. They sometimes understate the unprecedented gains in privacy protection that have also been achieved over the last half of the twentieth century. In many cases the legal system has laid a foundation for privacy protection through court decisions, state and federal legislation, and self-regulation. For example:

• tapping personal telephone calls without a warrant was not considered unconstitutional until 1967.

• national security surveillance gained considerable oversight in the post-Watergate era; during the Vietnam era millions of citizens were watched by federal authorities.

• important privacy protections were provided for electronic communications in 1986; and • although records have never been given constitutional protections, Congress has stepped in to protect privacy by passing legislation that includes the Fair Credit Reporting Act, the Privacy Act, and the Video Privacy Protection Act. In many instances, users of new technologies have taken their privacy into their own hands. They have demanded and availed themselves of powerful new technologies to protect their privacy. And individuals have found and used the avenues afforded them by new communications media to make vocal their demands for privacy. New technologies and standards that enable users to protect their privacy are on the way.

vii. The paper finds out about the new threats to information privacy that appear as the result of the emerging Big Data practices and methodologies in today's networked world. In particular, the collection and analysis of large-scale data from social networking sites challenge the traditional conceptualization of privacy. In response, a new conceptual framework is proposed to encompass three key dimensions of privacy in the Big Data context: information identifiability, information ephemerality, and information linkability.

viii. The paper identified three online privacy issues. And these are:

- Through 'Sponsored Stories,' Facebook users who clicked on 'like' buttons had pictures of themselves with an endorsement sent to their friends in a what looked like sponsored advertising (Kravets 2012).
- The travel site Orbitz tracks how users arrived at their site to prioritize search results: if a user arrived at Orbitz from a competitor's site, Orbitz may prioritize results based on price (Mattioli 2012). Similarly, Facebook mines users' browser history to target advertising.
- Verizon offers a service Precision Market In sights to business customers to mine Verizon's customer call and web browsing information to map where people are located and the types of services they purchase and use (Hill 2012).

4. CONCLUSION

In comparing consumers' judgments about right to privacy on the internet, this study directly supports the attempt to meet consumers' privacy expectations or their right to privacy on the internet considering the importance of privacy notices in managing privacy online, more research should extend this study to shed light on how consumers understand notices and how consumers' perceptions of privacy notices map to their privacy expectations, if at all.

5. RECOMMENDATION

An extensive study into “Right to Privacy on the Internet should be considered as tentative until the effect of the subject matter is fully understood.

6. FUTURE WORKS

This study focused on corporations and regulators as power holders that influence right to privacy on the internet as well as privacy attitudes and behaviours. However, scholars identify that privacy threats are increasingly emerging from the external environment that is beyond the control of corporations, consumers, and regulators (Ferrell, 2017). Hence, future research should consider the changing power dynamics caused by unauthorised and illegal entities such as hackers and data brokers. Privacy concerns are the most widely used factor or construct to predict privacy-related consumer behaviour. This study also highlights the importance of privacy empowerment, which is only nascent in the marketing scholarship. Future studies need to probe into factors that can augment or diminish privacy empowerment. Also, the relationship of empowerment with different behavioural outcomes needs to be further studied.

There are some limitations to the study. The sample was drawn from Australian consumers only. Therefore, the homogeneity of our sample can cause limitations in generalising findings. The cross-country or -culture differences can impact consumer privacy attitudes and behaviours (Chen et al., 2013). Hence, such aspects should be considered in future investigations. Also, this study used cross-sectional data that provides a “snapshot” of the phenomena under investigation at a specific time frame. With changing technological environment and regulatory policies and mechanisms, for instance, recent enactment of general data protection regulation, privacy issues can evolve over time and to enhance government regulation.

REFERENCES

1. Sheehan B. Kim, H. G. M. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy and Marketing*, *19*(1), 62–73. https://doi.org/10.1509/jppm.19.1.62.16949
2. Martin K. (2015). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy and Marketing*, *34*(2), 210–227. https://doi.org/10.1509/jppm.14.139
3. O’Connor N, L. A., and L. A. (2015). Privacy in the digital age. *Nature*, *497*(7449), 287. https://doi.org/10.1038/497287a
4. Chander A, L. M. (2014). *Introductory Note To United Nations General Assembly Resolution On The Right To Privacy In The Digital Age Author (s): Anupam Chander and Molly Land Source: International Legal Materials, Vol. 53, No. 4 (2014), pp. 727-731 Published by: America*. *53*(4), 727–731.
5. (Bidegain E et al., 2022)Anic, D. I., Budak J, R. E., V, R., V, S. and, & B, S. (2019). Extended model of online privacy concern: what drives consumers’ decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281
6.

7. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
8. Joseph, R. I. (1998). Privacy on the Internet: Whose Information Is It Anyway? *Jurimetrics*, *38*(4), 565–573. http://www.jstor.org/stable/29762571
9. Kang H, S. W. H. J. (2021). Teens' privacy management on video-sharing social media: the roles of perceived privacy risk and parental mediation. *Internet Research*, *32*(1), 312–334. https://doi.org/10.1108/INTR-01-2021-0005
10. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
11. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
12. (Anic et al., 2019)
13. Anic, D. I., Budak J, R. E., V, R., V, S. and, & B, S. (2019). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281
14. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
15. (Joseph, 1998)Anic, D. I., Budak J, R. E., V, R., V, S. and, & B, S. (2019). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281
16. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
17. Joseph, R. I. (1998). Privacy on the Internet: Whose Information Is It Anyway? *Jurimetrics*, *38*(4), 565–573. http://www.jstor.org/stable/29762571
18. Kang H, S. W. H. J. (2021). Teens' privacy management on video-sharing social media: the roles of perceived privacy risk and parental mediation. *Internet Research*, *32*(1), 312–334. https://doi.org/10.1108/INTR-01-2021-0005
19. (Kang H, 2021)
20. Anic, D. I., Budak J, R. E., V, R., V, S. and, & B, S. (2019). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281
21. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
22. Joseph, R. I. (1998). Privacy on the Internet: Whose Information Is It Anyway? *Jurimetrics*, *38*(4), 565–573. http://www.jstor.org/stable/29762571
23. Anic, D. I., Budak J, R. E., V, R., V, S. and, & B, S. (2019). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281
24. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069

25. Joseph, R. I. (1998). Privacy on the Internet: Whose Information Is It Anyway? *Jurimetrics*, *38*(4), 565–573. http://www.jstor.org/stable/29762571
26. Anic, D. I., Budak J, R. E., V, R., V, S. and, & B, S. (2019). Extended model of online privacy concern: what drives consumers' decisions? *Online Information Review*, *43*(5), 799–817. https://doi.org/10.1108/OIR-10-2017-0281
27. Bidegain E, Koldo, S. A. A. B. D., Zuberogoitia, A., E, A., & Rozas, I. (2022). Youth and online privacy: a cross-border study in the Basque Country. *Journal of Information, Communication and Ethics in Society*, *20*(1), 54–71. https://doi.org/10.1108/JICES-06-2021-0069
28. Joseph, R. I. (1998). Privacy on the Internet: Whose Information Is It Anyway? *Jurimetrics*, *38*(4), 565–573. http://www.jstor.org/stable/29762571
29. Kang H, S. W. H. J. (2021). Teens' privacy management on video-sharing social media: the roles of perceived privacy risk and parental mediation. *Internet Research*, *32*(1), 312–334. https://doi.org/10.1108/INTR-01-2021-0005
30. Stanaland J.S Andrea, L. O. M. and L. S. (2009). *Providing Parents with Online Privacy Information : Approaches in the US and the UK Author (s): ANDREA J . S . STANALAND , MAY O . LWIN and SUSANNA LEONG Source : The Journal of Consumer Affairs , Vol . 43 , No . 3 , Special Issue on Privacy Literacy —*. *43*(3), 474–494.