Eurasian Experiment Journal of Arts and Management (EEJAM) ISSN: 2992-412X

©EEJAM Publications Volume 7 Issue 3 2025

Privacy Laws in the Age of Social Media: A Communication Analysis

Maria Edet Umo

Faculty of Law Kampala International University Uganda
Email: umomaria@kiu.ac.ug

ABSTRACT

The evolution of social media has transformed digital communication, making personal data a valuable commodity. However, the increasing commercialization of user data has sparked concerns over privacy rights and legal protections. This paper examines privacy laws in the digital age, focusing on regulatory frameworks in the United Kingdom and the United States. Using a communication-centered approach, it explores how legislative developments, public awareness, and corporate strategies shape data protection policies. It also assesses the impact of key regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) in balancing user privacy and corporate interests. Through a critical analysis of communication theories, the study highlights the role of transparency, user consent, and stakeholder engagement in data governance. The findings emphasize the need for adaptive legal frameworks to address emerging privacy challenges in a rapidly evolving digital landscape.

Keywords: Privacy laws, social media, GDPR, CCPA, data protection, communication theory, digital privacy.

INTRODUCTION

Privacy laws have become increasingly important, particularly in light of developments in digital communication, social media, and the Internet. Personal data have become the digital equivalent of money, but it is nearly impossible to comprehend – let alone award value to – our own data trails, the digital crumbs we leave behind. It is our digital personas, the embodiment of our data, that are at stake in our digital world of surveillance capitalism, big data, and predictive analytics. The fact that it is tenable to exchange personal data for services also indicates a loss of control over our data. The act of relinquishing our privacy occurs mostly without any kind of explicit consent, nor do we receive full disclosure as to how our data are employed [1, 2]. The GDPR provides extensive safeguards and rights for the protection of personal data. Conversely, corporate actors acclaim such regulations and often self-honor their commitment to applicable laws. Conversely, compliance has a business rationale; for example, data protection is the new game in town. The impetus for this analysis is multifaceted. While aspects of privacy and the utilization of user data are cultural and hence nuanced by different constitutional approaches, human rights, legislative history, and social expectations, this paper focuses on the laws of the United Kingdom and the United States. Furthermore, this analysis also shifts its focus from the individual to larger-scale commercial and societal goals; that is, the ramifications of legal decisions not only for the individual plaintiff but also for the corporations that rely on big data and user data [3, 4].

Background and Rationale

Before the advent of social media, society operated without explicit privacy laws. However, algorithmic prediction technologies employed in social media platforms have commercialized user data and forensic inference, leading to calls for privacy protections. While the government has been slow or inconsistent in

enacting laws to expand legal privacy controls and government oversight, several privacy catastrophes have forced legislative changes to various consumer privacy laws. In the European Union, the General Data Protection Regulation replaced the 1995 EU Data Protection Directive. In the United States, California recently passed consumer privacy protections, and several other states have privacy laws moving through the legislative process. Here we take a communication approach to critically examine user data privacy as a multi-stakeholder issue. This starts with public, media, and industry awareness. Social media platforms have been described as 'walled gardens' where users cannot see over the walls. The Ambra Social Media Index aims to assess levels of privacy 'transparency' on social media platforms by considering a range of practices, namely social media platforms' interface with data protection, privacy interfaces, responses to access requests, data policies, and user agreements. The measures include ethical norms as well as legal and usability criteria. The monitoring examines more explicit data processing activities of social media platforms, as well as policy developments and public attitudinal data. The methodology is designed for longitudinal use and continuous development. Perfect transparency may never be reached as new analytical methods and posts' purposes emerge. The Ambra Social Media Index is unique in linking legal, ethical, and attitudinal measures, allowing continuous updates of repeatedly tested, validated, and refined measures reflecting the privacy views of the public and the current state of the art of policy development. This is necessary because, currently, extensive public consultation and continuous dialogue among multi-stakeholders seem necessary to efficiently contain the private, socially, and democratically harmful practices emerging on these platforms [5, 6].

Theoretical Framework

The communication-centered theory, or third-era theories of public relations, sees communication as the primary locus for understanding and influencing how regulation and lobbying are done in the policy cycle of law generation. These theories state that regulatory agendas are shaped by the claims raised in the media, and communication is a fundamental part of the process of legislation. Therefore, to approach communicational issues, these theories suggest an understanding of how diverse stakeholders understand themselves and the world, as well as the epistemic and ethical implications of the different forms of knowledge that they use in their social practices. Privacy, as a social construct, is best understood through evaluative methods and epistemic processes. One way to oversimplify and facilitate the inquiry on privacy is by addressing the regulatory discourses on privacy. Therefore, communications are economical because they concentrate on the most important social concerns of a given society; they are evaluative, as they display what a certain society believes to be right or wrong; and thus they are also ethical, promoting the rightness and universally agreed knowledge of the believer. The goal of third-era public relationships is to facilitate communication within this mix of knowledge and different interest groups and to see how communication practices can influence how larger societal decisions are made. These theories allow us to clarify the reasoning in favor of or against certain social issues and also call for transparent processes of legitimization of the discourses and their outcomes. If this approach is insufficient, the second-era audience-centered theories take situation-specific research and action in disorganized and complex public fundamentals, accounting for complexity in environmental contexts. The approach is mainly evaluative as it focuses on the stakeholders' understanding of privacy as a set of values and norms [7, 8].

Communication Theory

To develop a discourse on the role of communication in privacy law, we need to explore which communication theories have already been developed around privacy and social media. Multiple theories exist that can explain the communication between social media and its users. The operation of the Social Exchange Theory in user behavior and technology has been backed up extensively with research. The Privacy Calculus, an extension of Social Exchange Theory, links privacy concerns to surveillance awareness and risk perceptions by adding salience and severity as valuation factors. It is important as a base for other communication studies, but it becomes crucial for exploring law formation when communication strategies are added to the calculus. Just as the Privacy Calculus is a theoretical tool to explain privacy behavior, the Privacy Communication Framework can be and has been tested as a tool to understand privacy campaigns. Both theories assist researchers in understanding when, how, and why people consent or do not consent [9, 10]. Using communication theory to explain people's interactions with social media forms an excellent starting point to critically study the matter because both are core communication concepts. Several arguments have already been started that we will draw on in their next papers. But communication theory focuses on the social media user instead of the consumer and explores

their role in the privacy exchanges. Further, a variety of communication scholars have recently adopted the Privacy Communication Framework as a stepping stone for discourse about the direction privacy law needs to take in its treatment of deliverability. The Privacy Communication Framework's focus on "communication strategies" and "risk communication" can provide a helpful bridge between communication theory and the privacy challenges that need to be addressed by designing deliverability [11, 12].

Privacy Laws and Social Media

The use of social media is increasingly intertwined in many aspects of users' lives. This has led to questions about whether users are well protected under privacy legislation. Legitimate complaints and debates illustrate that not all laws seem to prevent privacy violations by companies. However, many of the privacy provisions that are in place stem from discussions and decisions from the pre-social media era. This present study aims to identify to what extent the legal privacy standards are still reaching - or capable of reaching - protection in the current digital era. This will result in legal analyses that provide insight into the relationship between privacy laws and the values that are in play on various social media platforms for users and platform owners [13, 14]. Legislation on privacy can be found in various areas of the world. Commonalities as well as differences are found between legislative frameworks. In Europe, an extensive right to privacy is deeply rooted both in the European Convention on Human Rights as well as in the various constitutions of the Member States. In this regard, the GDPR has a European basis. The GDPR is explicitly based on the right to privacy and the right to data protection and works as a low-threshold regulation. Lastly, we have non-European-oriented laws and regulations. The United States has sectoral laws - protecting specific groups or focusing on specific data types/categories. However, none amount to what is found in Europe. In Australia, there is an extensive data protection act, but the Australian Privacy Principles only list broad conditions for the legal processing of personal data rather than an in-depth data protection framework [15, 16]. Seen from a communication perspective, the whole regulatory setting can be captured based on three main axes: At the first level, platform owners or operating bodies can be found. They can help shape legal requirements and have to find ways to embed this into the platform. They can bend or change the law by using content policies and service terms and conditions. The degree of external laws, including privacy laws, that platform owners have to comply with depends on which international or national borders can be crossed by a platform and by platform users. In that regard already, network effects play a role in making privacy protections plural. For instance, the GDPR protects all persons in the European Union and this can result in partly shaping the privacy protection of EU-based internet platforms beyond the internal matters of ordinary citizens. On the second level, the powers of national data protection authorities and other supervisory authorities differ. At the third level, end users can turn to bodies outside the platform for enforcement of their privacy rights. The availability and influence of enforcement vary between North America, Australia, and various European countries [17, 18].

Overview of Privacy Laws

A significant number of privacy-related data protection legislations have been enacted worldwide that impact a range of social media operations. This paper provides a concise overview of key laws and their focus and draws attention to the differences manifest in country-specific laws, before concluding by examining the challenge (and associated gaps) of enforcing rules through compliance-based and often consent-focused measures. The General Data Protection Regulation in the European Union came into effect in May 2018 and was followed by the California Consumer Privacy Act in the USA in January 2020, complicating digital service access and offerings for European and US users, respectively. Organizations, irrespective of location, serving EU citizens have had to comply with GDPR's expansive data protection approach, ranking the EU and Ireland as important loci of privacy advocacy globally, as well as regulation [19, 20]. There are important distinctions between data protection laws worldwide in terms of scope, as well as substantive and procedural rights. For example, key differences between the GDPR and CCPA include access, correction, deletion, portability and processing limitations, opt-out commands and duration, and penalties. Given global data-sharing practices, there are consistent calls for interoperability across privacy approaches in all countries, as well as dynamic and evolving legal adaptations. This is, however, often balanced against corporate lobbying and influencer challenges. The proposal for the European Data Act is consistent with these ongoing calls. Many argue that users proactively consenting to data sharing, collection, and use are neither informed, free, nor power-balanced, thereby limiting user agency and rendering corporate social responsibility more important. Those critical of reliance on

corporate duties and roles to protect privacy argue that individual data protection cannot be ensured by private corporations alone. This is also typically based on the premise that data regulator support of privacy is tilted by corporate capture. Multiple privacy centers are active globally to develop user and consumer privacy approaches and laws. Privacy offices within global corporations also played a significant role in drafting legislation [21, 22].

Implications and Challenges

What could be the implications of privacy laws on social media, given audience expectations and the nature of the medium? Unregulated communication in a global medium does not remain unaffected by national interests and values. However, the notion of regulation raises several challenges, including the capacity to stipulate and enforce regulations about the behavior of platforms, intermediaries, providers, regulators, and the industry on the one hand and the audience on the other. Initial reflection might explain the absence of such regulations by the mere absence of international cooperation and the challenge regulation faces from technological development [23, 24]. With the institutions that are supposed to regulate the system, a range of challenges related to the enforcement of the laws and the level of compliance and trust in the law has only recently begun to be better understood. It is noted that privacy laws are likely to lead to more distrust and less use, as users change their behavior to protect themselves from the regulations.

Future Directions

By drawing from elements of social media's impact on users' privacy and privacy laws on social networks in various papers, this work has revealed the extent of the issue of lack of privacy laws. Through the use of a case study of a data scandal, it has shown the impact a lack of privacy regulation can have on individuals and stressed the importance of such laws. This is further supported when examining the model of communication theory about privacy and the way communication changes in a social media context. It suggests that, as a result, a new way of regulating communication and privacy is needed. The paper aimed to evaluate the need for adaptation in current privacy frameworks to ensure this increase in privacy is upheld. As this is a contemporary issue, a necessary implication of this examination is that it launches further research and analysis into current social media privacy frameworks. This need for privacy extends far beyond social media into other aspects of internet use and data storage, and so further uptake of this model would be beneficial in a variety of internet contexts. The potential for future research into the effect various stakeholders could have on the regulation of privacy laws, specifically the adaptation of laws in social media, is also extremely valid. Including advertisers, employees, and shareholders would allow a comprehensive network to be established. Finally, it would also be particularly worthwhile to tease out the way technology impacts rules. This type of research is just a starting point, as governments and companies are most likely already exploring ways of strategizing. Researchers and countries alike must draw on the expertise of not only existing data privacy lawyers and scholars but also current technology makers [25, 26].

CONCLUSION

As social media continues to redefine digital interactions, privacy laws must evolve to ensure adequate protection for users. This study has highlighted the significance of regulatory frameworks in addressing privacy concerns while acknowledging the complexities of enforcement and compliance. The interplay between communication, corporate responsibility, and user awareness underscores the need for transparent data practices. While laws such as GDPR and CCPA have made strides in enhancing data security, further research is required to refine legal measures and ensure ethical data usage. Future developments in privacy regulation should consider technological advancements, global data-sharing practices, and multi-stakeholder involvement. By fostering a dynamic approach to data governance, policymakers can create a balanced framework that protects individual privacy while enabling responsible innovation in the digital era.

REFERENCES

1. Babikian J. Navigating legal frontiers: exploring emerging issues in cyber law. Revista Espanola de Documentacion Cientifica. 2023 Dec 30;17(2):95-109.
2. Büchi M, Festic N, Latzer M. The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. Big Data & Society. 2022 Jan;9(1):20539517211065368.
3. Staunton C, Slokenberga S, Parziale A, Mascalzoni D. Appropriate safeguards and article 89 of the GDPR: considerations for biobank, databank and genetic research. Frontiers in genetics. 2022 Feb 18;13:719317. frontiersin.org

4. Torre D, Alferez M, Soltana G, Sabetzadeh M, Briand L. Modeling data protection and privacy: application and experience with GDPR. Software and Systems Modeling. 2021 Dec;20:2071-87. uni.lu
5. Stepenko V, Dreval L, Chernov S, Shestak V. EU personal data protection standards and regulatory framework. Journal of Applied Security Research. 2022 Apr 3;17(2):190-207. [HTML]
6. Vlahou A, Hallinan D, Apweiler R, Argiles A, Beige J, Benigni A, Bischoff R, Black PC, Boehm F, Céraline J, Chrousos GP. Data sharing under the General Data Protection Regulation: time to harmonize law and research ethics?. Hypertension. 2021 Apr;77(4):1029-35. ahajournals.org
7. Yang K, Liu F. Computer-aided design of visual communication expression with creativity as the core. Computer-Aided Design and Applications. 2022;19(1).
8. Mak AK, Chaidaroon SS, Poroli A, Pang A. Understanding organizational and socio-cultural contexts: A communicative constitutive approach to social license to operate among top Hong Kong companies. Public Relations Review. 2021 Sep 1;47(3):102055.
9. Hall K, Helmus B, Eymann T. How to Balance Privacy and (Health) Benefits: Privacy Calculus and the Intention to Use Health Tracking at the Workplace. International Journal of Human–Computer Interaction. 2024 Jul 17:1-8. [HTML]
10. Shi J, Yuan R, Yan X, Wang M, Qiu J, Ji X, Yu G. Factors influencing the sharing of personal health data based on the integrated theory of privacy calculus and theory of planned behaviors framework: results of a cross-sectional study of Chinese patients in the Yangtze River Delta. Journal of Medical Internet Research. 2023 Jul 6;25:e46562. jmir.org
11. Harrigan M, Feddema K, Wang S, Harrigan P, Diot E. How trust leads to online purchase intention founded in perceived usefulness and peer communication. Journal of Consumer Behaviour. 2021 Sep;20(5):1297-312. qut.edu.au
12. Hwang J, Eves A, Stienmetz JL. The impact of social media use on consumers' restaurant consumption experiences: A qualitative study. Sustainability. 2021 Jun 9;13(12):6581.
13. Marx J, Mirbabaie M. The Investigator's Dilemma-A Review of Social Media Analytics Research Ethics in Information Systems. Australasian Journal of Information Systems. 2022 Jul 2;26. acs.org.au
14. Sahebi S, Formosa P. Social media and its negative impacts on autonomy. Philosophy & technology. 2022 Sep;35(3):70.
15. Hasal M, Nowaková J, Ahmed Saghair K, Abdulla H, Snášel V, Ogiela L. Chatbots: Security, privacy, data protection, and social aspects. Concurrency and Computation: Practice and Experience. 2021 Oct 10;33(19):e6426. wiley.com
16. Kretschmer M, Pennekamp J, Wehrle K. Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. ACM Transactions on the Web (TWEB). 2021 Jul 15;15(4):1-42. jpennekamp.de
17. Lawlor RT. The impact of GDPR on data sharing for European cancer research. The Lancet Oncology. 2023 Jan 1;24(1):6-8.
18. Van Bekkum M, Borgesius FZ. Using sensitive data to prevent discrimination by artificial intelligence: Does the GDPR need a new exception?. Computer Law & Security Review. 2023 Apr 1;48:105770.
19. Makulilo AB. Privacy and data protection in Africa: a state of the art. International Data Privacy Law. 2012 Aug 1;2(3):163-78.
20. Calzada I. Citizens' data privacy in china: The state of the art of the personal information protection law (pipl). Smart Cities. 2022 Sep 8;5(3):1129-50.
21. Andrew J, Baker M. The general data protection regulation in the age of surveillance capitalism. Journal of Business Ethics. 2021 Jan;168:565-78.
22. Almeida D, Shmarko K, Lomas E. The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. AI and Ethics. 2022 Aug;2(3):377-87.
23. Schiller HI. The privatization and transnationalization of culture. InCultural politics in contemporary America 2022 Nov 30 (pp. 317-332). Routledge.
24. Schneider V, Werle R. International regime or corporate actor? The European Community in telecommunications policy. InThe political economy of communications 2023 Oct 20 (pp. 77-106). Routledge.

25. Quach S, Thaichon P, Martin KD, Weaven S, Palmatier RW. Digital technologies: tensions in privacy and data. Journal of the Academy of Marketing Science. 2022 Nov;50(6):1299-323. springer.com
26. Fox G, Clohessy T, van der Werff L, Rosati P, Lynn T. Exploring the competing influences of privacy concerns and positive beliefs on citizen acceptance of contact tracing mobile applications. Computers in Human Behavior. 2021 Aug 1;121:106806. sciencedirect.com

CITE AS: Maria Edet Umo. (2025). Privacy Laws in the Age of Social Media: A Communication Analysis. Eurasian Experiment Journal of Arts and Management 7(3):53-58