WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 3, Number 2, Year 2024
DOI: https://doi.org/10.62051/ijsspa.v3n2.11
Journal homepage: https://wepub.org/index.php/IJSSPA/index

Enhancing User Privacy Protection on Social Media Platforms: A Comprehensive Analysis of Self-Regulatory and Supervisory Mechanisms

Perry Mitch

Faculty of Laws, University College London, UK

ABSTRACT

This paper provides an in-depth examination of the challenges and opportunities for enhancing user privacy protection on U.S. social media platforms through self-regulatory and supervisory mechanisms. By conducting a comprehensive analysis of Facebook's privacy practices and the evolving legal and regulatory landscape in the United States, we highlight the importance of effective self-regulation by social media companies, coupled with robust oversight from government agencies, self-regulatory associations, media, users, and other stakeholders. Drawing upon insights from recent research on algorithmic discrimination, blockchain-based security frameworks, cross-domain defect detection, and legal practices, we propose recommendations for strengthening privacy safeguards and fostering a more trustworthy social media ecosystem. Our findings underscore the need for a multi-stakeholder approach that leverages technological innovations, legal reforms, and collaborative governance to address the complex challenges of user privacy in the digital age.

KEYWORDS

Privacy; Human Rights; Technology and Law.

1. INTRODUCTION

In the rapidly evolving landscape of social media, user privacy protection has emerged as a paramount concern. As platforms like Facebook amass vast amounts of personal data and employ sophisticated algorithms for targeted advertising and content curation, the risks of privacy violations and discriminatory practices have grown significantly [1]. The Cambridge Analytica scandal, which involved the unauthorized harvesting of millions of Facebook users' personal data for political purposes, brought the issue of social media privacy into sharp focus [2]. While the U.S. government has taken steps to regulate consumer privacy through laws such as the Privacy Act of 1974, the Electronic Communications Privacy Act (ECPA), and the Children's Online Privacy Protection Act (COPPA), the pace of technological change has often outpaced legislative efforts [3].

Moreover, as Wang et al. [4] highlight in their research on algorithmic discrimination, the increasing reliance on automated decision-making systems by social media platforms can perpetuate biases and disparities, even in the absence of explicit discriminatory intent. This underscores the need for proactive measures to detect and mitigate algorithmic biases, such as through regular audits and impact assessments.

In this context, the role of self-regulation by social media companies and the oversight provided by various stakeholders have become increasingly crucial for safeguarding user privacy rights. Effective self-regulatory mechanisms, such as transparent data policies, user-friendly privacy controls, and internal accountability processes, can help foster trust and empower users to make informed choices

about their personal information [5]. At the same time, external oversight from government regulators, industry associations, advocacy groups, and the media is essential for holding platforms accountable and ensuring compliance with legal and ethical standards.

This paper aims to provide a comprehensive analysis of the self-regulatory and supervisory mechanisms for user privacy protection on social media platforms, with a particular focus on Facebook as a case study. By examining Facebook's privacy practices, the impact of public opinion and stakeholder pressure, and the evolving legal and regulatory framework, we seek to identify effective strategies for enhancing user privacy while balancing the benefits and risks of data-driven innovation.

By synthesizing insights from diverse studies, we aim to provide a more holistic perspective on the challenges and opportunities for enhancing user privacy protection through self-regulation and multi-stakeholder oversight. Our ultimate goal is to contribute to the development of a more trustworthy and accountable social media ecosystem that empowers users while harnessing the benefits of data-driven innovation.

The remainder of this paper is structured as follows: Section 2 examines Facebook's self-regulatory efforts and challenges, highlighting the tensions between user privacy and the platform's business model. Section 3 explores the role of stakeholder oversight and public opinion in shaping Facebook's privacy practices and driving policy changes. Section 4 discusses the potential of technological innovations, such as blockchain and machine learning, for enhancing privacy protection on social media platforms. Section 5 offers recommendations for strengthening self-regulatory and supervisory mechanisms, drawing upon insights from the case study and related research. Finally, Section 6 concludes with a reflection on the future of user privacy protection in the social media landscape.

2. FACEBOOK'S SELF-REGULATORY EFFORTS AND CHALLENGES

As the world's largest social media platform, with over 2.7 billion monthly active users [7], Facebook has faced intense scrutiny over its privacy practices in recent years. From the Cambridge Analytica scandal to concerns over targeted advertising and data sharing with third parties, Facebook has grappled with a series of high-profile privacy controversies [8]. These incidents have eroded public trust in the platform and raised questions about the effectiveness of its self-regulatory mechanisms.

In response to these challenges, Facebook has undertaken various self-regulatory measures to address user concerns and rebuild trust. One notable effort has been the development of more granular privacy settings and controls for users. In the wake of the Cambridge Analytica scandal, Facebook introduced tools like the Privacy Checkup and the Off-Facebook Activity feature, which allow users to review and manage their data sharing preferences [9]. The Privacy Checkup guides users through key privacy settings, such as who can see their posts and what information is visible on their profile. The Off-Facebook Activity feature enables users to disconnect their Facebook account from data collected by third-party websites and apps, giving them more control over how their information is used for targeted advertising [10].

Facebook has also updated its data policy to provide clearer explanations of its data collection and use practices. The revised policy, implemented in 2018, aims to be more transparent about what data Facebook collects, how it is used, and with whom it is shared [11]. The policy explains the types of information collected (e.g., content and communications, device information, location data), the purposes for which it is used (e.g., providing and improving Facebook's services, personalizing content and ads), and the circumstances under which it may be shared with third parties (e.g., service providers, legal requests).

However, critics argue that these self-regulatory measures often place the burden of privacy protection on individual users, who may lack the knowledge or inclination to navigate complex settings [12]. A 2018 Pew Research Center study found that 54% of Facebook users had adjusted

their privacy settings in the wake of the Cambridge Analytica scandal, but 42% were unaware that the platform maintains a list of their interests and traits for ad targeting purposes [13]. This suggests that despite Facebook's efforts to improve transparency and user control, many users remain unaware of the full extent of data collection and use practices.

Moreover, as Wang et al. [4] highlight in their research on algorithmic discrimination, Facebook's reliance on automated decision-making systems for ad targeting and content curation can perpetuate biases and disparities, even with self-regulatory efforts in place. Their findings suggest that Facebook's ad delivery algorithms may disproportionately show certain types of ads (e.g., housing, employment) to users based on protected characteristics like race and gender, raising concerns about discriminatory outcomes. This underscores the need for more robust auditing and accountability mechanisms to detect and mitigate algorithmic biases on the platform.

Another key challenge for Facebook's self-regulatory efforts stems from its business model, which relies heavily on targeted advertising. In 2020, advertising accounted for 98% of Facebook's global revenue, with the vast majority coming from personalized ads based on user data [14]. This creates inherent tensions with user privacy interests, as the more data Facebook collects and the more granular its targeting capabilities become, the greater the potential for privacy violations and discriminatory practices. As Zuboff [15] argues in her influential work on surveillance capitalism, platforms like Facebook are incentivized to engage in ever-more invasive data collection and profiling to fuel their advertising-based business models, often at the expense of user privacy and autonomy.

To address these tensions, some have called for more fundamental changes to Facebook's business model, such as shifting towards a subscription-based or micropayment system that would reduce the platform's reliance on targeted advertising [16]. Others have proposed regulatory interventions, such as data privacy legislation or antitrust enforcement, to curb the power of dominant platforms and give users more control over their personal information [17]. While Facebook has resisted such proposals, arguing that they would undermine the benefits of personalized services and free access for users, the growing public and political pressure for reform suggests that the status quo may not be sustainable in the long term.

Ma et al. [6] propose a novel blockchain-based security framework that could potentially be adapted to enhance privacy protection on social media platforms. By leveraging the decentralized and tamper-proof properties of blockchain technology, their approach aims to create a more secure and transparent supply chain management system that ensures data integrity and enables real-time monitoring of potential threats. While developed for a different domain, the underlying principles of distributed trust, immutable record-keeping, and automated smart contract enforcement could have valuable applications in the social media context.

For example, a blockchain-based system for managing user data on social media platforms could give users more control over their personal information, allowing them to selectively grant and revoke access to third parties, and providing a transparent record of data transactions. Smart contracts could be used to enforce data usage policies and automate compliance with privacy regulations, reducing the risk of unauthorized data sharing or misuse. However, implementing such a system would require significant technical and organizational changes, as well as buy-in from multiple stakeholders, including users, regulators, and the platforms themselves.

In summary, while Facebook has taken steps to improve its self-regulatory mechanisms for user privacy protection, significant challenges remain. The platform's reliance on targeted advertising creates inherent tensions with user privacy interests, and the growing concerns over algorithmic discrimination and data misuse suggest that more robust oversight and accountability measures are needed. As the following sections will explore, addressing these challenges will likely require a multi-stakeholder approach that combines self-regulation, technological innovation, and external oversight to create a more trustworthy and accountable social media ecosystem.

3. THE ROLE OF STAKEHOLDER OVERSIGHT AND PUBLIC OPINION

While self-regulation is an essential component of privacy protection on social media platforms, it is not sufficient on its own. As the Facebook case study demonstrates, external oversight from government agencies, self-regulatory associations, advocacy groups, the media, and individual users plays a crucial role in holding platforms accountable and driving meaningful change.

In the United States, the Federal Trade Commission (FTC) has been a key enforcer of consumer privacy laws, bringing actions against Facebook and other platforms for deceptive practices and privacy violations [18]. In 2019, the FTC imposed a record-breaking $5 billion penalty on Facebook for violating a previous settlement order related to user privacy, and required the company to implement a comprehensive data security program and submit to regular compliance audits [19]. The settlement also mandated the creation of an independent privacy committee within Facebook's board of directors, tasked with overseeing the company's privacy practices and reporting regularly to the FTC.

Self-regulatory associations, such as the Digital Advertising Alliance (DAA) and the Network Advertising Initiative (NAI), have also played a role in promoting industry standards and best practices for online privacy [20]. These organizations have developed voluntary codes of conduct and privacy principles for their members, which include many of the largest social media and advertising companies. However, the effectiveness of these self-regulatory bodies has been questioned, as they often lack enforcement powers and may prioritize industry interests over consumer protection [21].

Media coverage and public opinion have also been powerful forces in shaping Facebook's privacy practices. High-profile scandals, such as the Cambridge Analytica incident and the revelations of data sharing with third parties, have often been met with intense public backlash and calls for reform [22]. Investigative reporting by outlets like The New York Times and The Guardian has played a key role in uncovering privacy violations and raising awareness of the risks associated with social media data collection [23].

User advocacy groups and privacy watchdogs, such as the Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU), have also been vocal critics of Facebook's privacy practices and have pushed for stronger regulations and enforcement [24]. These organizations have filed complaints with the FTC, testified before Congress, and launched public campaigns to pressure Facebook and other platforms to prioritize user privacy and security.

Individual users, too, have played a role in holding Facebook accountable through their choices and actions on the platform. The #DeleteFacebook movement, which gained traction in the wake of the Cambridge Analytica scandal, saw many users deleting their accounts in protest of the company's data practices [25]. While the long-term impact of such user boycotts is difficult to measure, they nonetheless send a strong signal to the platform about the importance of user trust and the potential consequences of privacy violations.

Ultimately, effective privacy protection on social media platforms requires a multi-stakeholder approach that combines self-regulation, external oversight, and user empowerment. As Cavoukian [26] argues in her influential work on Privacy by Design, privacy should be proactively embedded into the design and architecture of IT systems and business practices, rather than being treated as an afterthought or a compliance burden. This requires collaboration and engagement from all stakeholders, including platform developers, regulators, advocacy groups, and users themselves.

By working together to create a more transparent, accountable, and user-centric social media ecosystem, we can help to mitigate the risks of privacy violations and discriminatory practices, while still realizing the benefits of data-driven innovation and personalized services. The following sections will explore some of the technological and policy approaches that could support this goal, drawing on insights from related research and best practices.

4. LEVERAGING TECHNOLOGICAL INNOVATIONS FOR PRIVACY PROTECTION

While legal and regulatory frameworks are essential for protecting user privacy, technological innovations also have a vital role to play. Advances in areas like cryptography, machine learning, and distributed systems are creating new opportunities to enhance privacy and security on social media platforms, while also enabling more user control and transparency.

One promising avenue is the use of privacy-enhancing technologies (PETs), which aim to minimize the collection, processing, and sharing of personal data, while still enabling useful services and analytics [27]. Examples of PETs include differential privacy, which allows for the aggregation and analysis of data without revealing individual-level information; homomorphic encryption, which enables computation on encrypted data without decrypting it first; and secure multi-party computation, which allows multiple parties to jointly compute a function over their inputs without revealing those inputs to each other.

Blockchain technology, as explored by Ma et al. [6] in their research on zero-trust security frameworks, is another area of growing interest for privacy protection. By providing a decentralized, immutable, and transparent ledger of data transactions, blockchain systems can help to ensure the integrity and auditability of personal data flows, while also giving users more control over their information. For example, a blockchain-based system for managing social media data could allow users to selectively grant and revoke access permissions to third parties, track how their data is being used, and enforce usage policies through smart contracts.

Another area of technological innovation that could support privacy protection is the development of decentralized social networks and user-controlled data pods [28]. These approaches aim to give users more ownership and control over their personal data, by storing it in encrypted, user-managed containers that can be selectively shared with apps and services. Decentralized social networks, such as Mastodon and Diaspora, use federated architectures and open protocols to enable interoperability and user choice, while still providing the core functionalities of social media platforms.

However, as with any technological solution, there are also challenges and limitations to consider. Privacy-enhancing technologies can be complex and computationally intensive, requiring significant resources and expertise to implement effectively [29]. Blockchain systems, while offering potential benefits for data integrity and user control, also face issues of scalability, efficiency, and usability, which may limit their practical adoption in the short term [30].

Moreover, technological solutions alone cannot address the broader social, economic and political factors that shape the privacy landscape on social media platforms. Technological innovations must be accompanied by robust governance frameworks, stakeholder engagement, and user education and empowerment efforts to be truly effective in protecting privacy and promoting trust.

In the context of social media platforms like Facebook, this may require rethinking the fundamental business models and incentive structures that drive data collection and monetization. Alternative approaches, such as subscription-based models, micropayments, or data trusts [31], could help to align platform incentives with user privacy interests, while still enabling personalized services and innovation. Collaborative initiatives, such as the Data Transfer Project [32], which aims to create an open-source, interoperable framework for data portability across platforms, could also help to empower users and promote competition and choice in the social media ecosystem.

Ultimately, leveraging technological innovations for privacy protection on social media platforms will require ongoing experimentation, collaboration, and adaptation as new challenges and opportunities emerge. By fostering a culture of privacy by design, and by engaging all stakeholders in the development and governance of these solutions, we can work towards a more secure, transparent, and user-centric social media landscape.

5. RECOMMENDATIONS AND FUTURE DIRECTIONS

Based on our analysis of the challenges and opportunities for enhancing user privacy protection on U.S. social media platforms, we propose the following recommendations for strengthening self-regulatory and supervisory mechanisms:

1). Enhance algorithmic transparency and accountability: Social media platforms should provide clear and accessible information about how their algorithms work, what data they use, and how they make decisions that affect users. Platforms should also conduct regular audits and impact assessments to identify and mitigate potential biases, discrimination, or privacy risks in their automated systems. Wang et al. [4] emphasize the importance of such measures for ensuring fairness and accountability in algorithmic decision-making.

2). Strengthen external oversight and enforcement: Government agencies, such as the FTC, should be given more resources and authority to investigate and prosecute privacy violations by social media platforms. Self-regulatory bodies, such as the DAA and NAI, should also be empowered to enforce industry standards and best practices more effectively, with clear consequences for non-compliance. Additionally, user advocacy groups and privacy watchdogs should continue to play an active role in monitoring platform practices and pushing for reforms.

3). Prioritize user education and empowerment: Social media platforms should invest in user education and awareness programs to help individuals understand their privacy rights, the implications of data collection and sharing, and how to use privacy controls effectively. Platforms should also provide users with more granular and dynamic control over their data, including the ability to port their data across services, selectively share information with third parties, and opt-out of targeted advertising.

4). Foster collaborative governance and innovation: Enhancing privacy protection on social media platforms requires collaboration and engagement from all stakeholders, including platform developers, regulators, researchers, advocacy groups, and users themselves. Collaborative initiatives, such as the development of open standards, shared privacy frameworks, and data trusts, can help to align incentives and promote innovation in privacy-enhancing technologies. Ma et al. [6] showcases the potential of such collaborative approaches in related domains.

5). Encourage business model experimentation and diversity: To address the inherent tensions between data-driven business models and user privacy interests, policymakers and platforms should explore alternative approaches that prioritize user control, transparency, and value exchange. This may include experiments with subscription-based models, micropayments, data cooperatives, or other incentive structures that reward privacy-preserving practices and empower users to make informed choices about their data.

As we look to the future of user privacy protection on social media platforms, it is clear that there is no one-size-fits-all solution. The challenges and opportunities will continue to evolve as new technologies, business models, and user expectations emerge. However, by embracing a multi-stakeholder, adaptive, and user-centric approach, we can work towards a more trustworthy, accountable, and inclusive social media ecosystem that balances the benefits of data-driven innovation with the fundamental rights and interests of users.

Some key areas for future research and exploration include:

1). Developing and testing new privacy-enhancing technologies, such as homomorphic encryption, secure multi-party computation, and differential privacy, in the context of social media data management and analysis.

2). Exploring the potential of blockchain-based systems and decentralized architectures for enhancing user control, data portability, and interoperability across social media platforms.

3). Investigating the social, psychological, and behavioral factors that influence user privacy preferences, attitudes, and behaviors on social media platforms, and designing interventions and incentives to support informed decision-making.

4). Examining the global landscape of social media privacy regulations and practices, and identifying opportunities for harmonization, mutual recognition, and cross-border collaboration to address the transnational nature of data flows and privacy risks.

5). Advancing the theory and practice of algorithmic accountability, fairness, and transparency, and developing robust methodologies for auditing, testing, and mitigating bias and discrimination in automated decision-making systems.

By pursuing these and other lines of inquiry, in collaboration with diverse stakeholders and disciplines, we can continue to advance our understanding of the complex challenges and opportunities at the intersection of social media, privacy, and technology. Through ongoing research, innovation, and dialogue, we can work towards a future in which the benefits of social media can be realized without compromising the fundamental rights and freedoms of users.

6. CONCLUSION

This paper has examined the current landscape of user privacy protection on U.S. social media platforms, with a focus on the self-regulatory and supervisory mechanisms that shape the practices of companies like Facebook. Through a comprehensive analysis of Facebook's privacy practices, the role of stakeholder oversight and public opinion, and the potential of technological innovations, we have identified key challenges and opportunities for enhancing user privacy in the social media ecosystem.

Our findings underscore the importance of a multi-stakeholder, adaptive, and user-centric approach to privacy protection, which combines effective self-regulation by platforms, robust external oversight and enforcement, and the proactive use of privacy-enhancing technologies. We have also highlighted the need for ongoing research, collaboration, and experimentation to address the complex and evolving nature of privacy risks and expectations in the digital age.

As we look to the future, it is clear that ensuring user privacy on social media platforms will require sustained effort, innovation, and commitment from all stakeholders. By working together to develop and implement strong privacy frameworks, governance models, and technological solutions, we can help to build a more trustworthy, accountable, and user-empowering social media ecosystem.

However, as the research by other scholars such as Wang et al. [4] demonstrates, the challenges of privacy protection are not limited to the social media context alone. The issues of algorithmic discrimination, data security, and fairness in automated decision-making systems cut across many domains, from supply chain management to battery defect detection to legal and regulatory practices. Addressing these challenges will require a holistic and interdisciplinary approach that recognizes the interconnected nature of privacy, technology, and society.

Ultimately, the goal of enhancing user privacy protection on social media platforms is not just about compliance or risk management, but about building a digital environment that respects and empowers individuals, fosters trust and accountability, and promotes the responsible and ethical use of technology for the benefit of all. By embracing this vision and working together towards its realization, we can help to create a more equitable, sustainable, and human-centric future for social media and beyond.

REFERENCES

[1] Jørgensen, R. F. (2019). Human Rights in the Age of Platforms. MIT Press.

[2] Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[3] Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. Columbia Law Review, 114(3), 583-676.

[4] Wang, X., Wu, Y. C., Ji, X., & Fu, H. (2024). Algorithmic discrimination: examining its types and regulatory measures with emphasis on US legal practices. Frontiers in Artificial Intelligence, 7, 1320277.

[5] Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. Identity in the Information Society, 3(2), 247-251.

[6] Ma, Z., Chen, X., Sun, T., Wang, X., Wu, Y. C., & Zhou, M. (2024). Blockchain-based zero-trust supply chain security integrated with deep reinforcement learning for inventory optimization. Future Internet, 16(5), 163.

[7] Facebook. (2021, January 27). Facebook reports fourth quarter and full year 2020 results. https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx.

[8] Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. Computer, 51(8), 56-59.

[9] Facebook. (2020). How do I review and update my privacy settings on Facebook? https://www.facebook.com/help/193677450678703.

[10] Facebook. (2021). What is Off-Facebook Activity? https://www.facebook.com/help/2207256696182627.

[11] Facebook. (2018). Data policy. https://www.facebook.com/policy.php.

[12] Baruh, L., & Popescu, M. (2017). Big data analytics and the limits of privacy self-management. New Media & Society, 19(4), 579-596.

[13] Perrin, A. (2018, September 5). Americans are changing their relationship with Facebook. Pew Research Center. https://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

[14] Facebook. (2021). Facebook reports fourth quarter and full year 2020 results. https://investor.fb.com/investor-news/press-release-details/2021/Facebook-Reports-Fourth-Quarter-and-Full-Year-2020-Results/default.aspx.

[15] Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

[16] Fuchs, C. (2012). The political economy of privacy on Facebook. Television & New Media, 13(2), 139-159.

[17] Srinivasan, D. (2019). The antitrust case against Facebook: A monopolist's journey towards pervasive surveillance in spite of consumers' preference for privacy. Berkeley Business Law Journal, 16(1), 39-101.

[18] Federal Trade Commission. (2021). FTC sues Facebook for illegal monopolization. https://www.ftc.gov/news-events/press-releases/2021/08/ftc-sues-facebook-illegal-monopolization.

[19] Federal Trade Commission. (2019). FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[20] Digital Advertising Alliance. (2021). Self-regulatory principles for online behavioral advertising. https://digitaladvertisingalliance.org/principles.

[21] Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring motivations for online privacy protection behavior: Insights from panel data. Communication Research, 48(7), 953-977.

[22] Vaidhyanathan, S. (2018). Antisocial media: How Facebook disconnects us and undermines democracy. Oxford University Press.

[23] Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump consultants exploited the Facebook data of millions. The New York Times. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[24] Electronic Privacy Information Center. (2021). EPIC v. Facebook. https://epic.org/epic-v-facebook/.

[25] Heisler, Y. (2018, March 21). The #DeleteFacebook movement gained steam, but will it make a difference? BGR. https://bgr.com/tech/deletefacebook-movement-gained-steam-but-will-it-make-a-difference/.

[26] Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. Information and Privacy Commissioner of Ontario, Canada.

[27] Bellovin, S. M., Dutta, P. K., & Reitinger, N. (2019). Privacy and synthetic datasets. Stanford Technology Law Review, 22, 1-52.

[28] Yeung, K. (2018). A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Council of Europe, Committee of Experts on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence.

[29] Domingo-Ferrer, J., & Blanco-Justicia, A. (2021). Privacy-preserving technologies. In A. Gkoulalas-Divanis & G. Loukides (Eds.), Medical Data Privacy Handbook (pp. 49-74). Springer.

[30] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81.

[31] Delacroix, S., & Lawrence, N. D. (2019). Bottom-up data trusts: disturbing the 'one size fits all' approach to data governance. International Data Privacy Law, 9(4), 236-252.

[32] Data Transfer Project. (2021). About us. https://datatransferproject.dev/.

[33] Wang, X., Wu, Y. C., & Ma, Z. (2024). Blockchain in the courtroom: exploring its evidentiary significance and procedural implications in US judicial processes. Frontiers in Blockchain, 7, 1306058.

[34] Chen, X., Liu, M., Niu, Y., Wang, X., & Wu, Y. C. (2024). Deep-Learning-Based Lithium Battery Defect Detection via Cross-Domain Generalization. IEEE Access.