International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 5, Sep-Oct 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Data Privacy and Protection in the Digital Age: Challenges, Regulatory Responses and Implications for Ghana

Jessica Mawule Adotevie

Assistant Librarian, Library Department, Family Health University, Accra, Ghana

ABSTRACT

Data privacy and data protection matter greatly to both individuals and businesses. As the internet continues to expand and influence nearly every area of our lives, the massive volumes of personal information created, collected, and shared have raised serious concerns about individual privacy, security, and data ethics. This paper examines the mechanisms in place for safeguarding data and ensuring the privacy of internet users, the concerns internet users have regarding privacy, and the benefits and challenges associated with internet usage and the protection of data and privacy. It reviews data privacy and security risks, regulatory frameworks, Ghana's Data Protection Act, 2012 (Act 843), challenges to effective protection, and measures available to organisations and users. The discussion highlights data breaches, human error, legal complexity, resource constraints, and rapid technological advancements. It concludes that openness about how user data is acquired, handled, and shared promotes confidence among users, while effective data protection requires organisations, governments, and individuals to work together.

KEYWORDS: *Data Privacy, Data Protection, Internet Users, Cybersecurity, Ghana, Data Protection Act.*

How to cite this paper: Jessica Mawule Adotevie "Data Privacy and Protection in the Digital Age: Challenges, Regulatory Responses and Implications for Ghana" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-5, October 2026, pp.1477-1485, URL: www.ijtsrd.com/papers/ijtsrd142223.pdf

IJTSRD142223

Copyright © 2026 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

1. INTRODUCTION

In our increasingly linked and digitised world, one of the most serious and controversial concerns of our day is data protection and internet user privacy. As the internet continues to expand and influence practically every area of our lives, the massive volumes of personal information created, gathered, and disseminated have sparked serious concerns about individual privacy, security, and data ethics. Since the early days of the internet, the digital world has seen amazing change. What began as a simple network for information exchange has grown into a complex ecosystem that includes social media platforms, e-commerce websites, mobile apps, and the Internet of Things (IoT). The amount of data collected daily has reached startling dimensions as a result of this progression. Every click, tap, or swipe creates a digital imprint, from our internet searches and social media postings to our financial transactions and health information. Despite the significance of privacy in the digital age, people, including those with severe privacy concerns, frequently exchange their personal information for online services and products (Carrascal et al., 2013).

Privacy concerns have gotten stronger as the Internet's expansion has resulted in ubiquitous data collection and usage practices. The Internet has profoundly altered many parts of our lives, including how we work, consume, and interact. While this has had significant benefits for society, the expanding influence of the Internet and technology has always been related to privacy issues and the gathering and use of personal information. Individual privacy risks posed by these technologies have been well recognised. In recent years, sensitive personal data has been taken illegally and misused in a number of data breaches. Recently, almost 150 million people's sensitive personal information, including credit scores, were compromised in the 2017 Equifax data breach (Zou and Schaub, 2018), and around 87 million Facebook users were impacted by the Cambridge Analytica data scandal in 2018 (Revell, 2018).

This expanding data flood has raised significant problems and difficulties, the most pressing of which is the preservation of human privacy. Today's internet users confront several privacy dangers, such as data

breaches, identity theft, online tracking, and spying. As a result, there is an increasing need to protect the personal information that people entrust to online platforms and service providers. Privacy concerns have emerged as one of the most pressing issues in the digital age, affecting researchers, consumers, corporations, practitioners, and policymakers alike. Acquisti and Gross (2009) established the risk to individual privacy by deducing identities (i.e., social security numbers) from ostensibly "anonymized" data. Other research found that Facebook Likes and face photos might be used to infer sensitive personal information such as sexual orientation (Kosinski et al., 2013; Wang and Kosinski, 2018).

In response to these issues, the legal and regulatory landscape surrounding data protection and privacy is continually developing. Significant initiatives, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), have established major precedents by giving consumers greater control over their personal data. These legislations have required organisations to be more transparent about their data practices and to give users means to view, update, or delete their data.

2. Conceptual Background

Data privacy and data protection are extremely important to both individuals and businesses. In various countries, the idea of privacy has been recognised as a basic human right of individuals, as privacy is crucial to a free society. Data privacy is also viewed as an individual's right to choose who has access to their personal information, what personal information is disclosed, and the protection of that information from unauthorised parties. Data protection, on the other hand, is regarded as a company's obligation to protect its consumers' personal information against unauthorised use. It entails enforcing policies to avoid abuse or unauthorized access to users' personal information, as well as employing defensive measures against all weaknesses in their data gathering and storage system.

From history to the present era, the notion of privacy has played an essential part in social, political, economic, and theological research. The notion of privacy can be found in Aristotle's writings on politics, as well as John Locke's works on public and private property in the 1600s, where the writers distinguish between public and private areas and indicate the latter as a facet of privacy (DeCew, 2016). As civilisation progressed, social and political developments resulted in the acknowledgement of additional rights, one of which was the "right to be left alone" (Cooley, 1879). According to Samuel D. Warren and Louis D. Brandeis, every individual is entitled to privacy of body and mind, and this right is enforceable, a right recognised today as the right to privacy (Warren & Brandeis, 1890).

Westin, considered the father of the current notion of privacy, described it as an individual's, a group's or an organisation's right to control when, how, and to what degree information about them can be shared with others (Westin, 1967). The notion of data protection and privacy has a long history. It may be traced back to ancient civilisations, when people used various methods to protect personal information, such as encryption and sealed letters. However, when data became more freely available and sensitive in the digital age, additional issues arose.

However, traditional definitions and understandings of privacy developed before the introduction of the internet are unprepared to deal with technological issues (Austin, 2003). The introduction and accessibility of the internet broadened the scope of information privacy or data privacy to include the digital environment.

Information privacy is the desire of an individual to retain control over what information about them may be circulated on digital platforms (Jeff Smith, 2011). Information privacy refers to the ability of individuals or organisations to control the collection, use, and dissemination of their personal information (Wang, 2019). With the increasing amount of data being collected and shared online, concerns about information privacy have become more prominent.

Data protection is the legal control exercised over a third party's inappropriate access and use of an individual's personal information. This phrase was first used in Europe to refer to privacy-protection laws (Swire and Ahmad, 2012). Data protection is also seen as the process of safeguarding important information from corruption, compromise, or loss. It is a set of strategies and processes that can be used to secure the privacy, availability, and integrity of data (Cloudian, 2023). Data protection is vital for any organisation that collects, handles, or stores sensitive data. A successful strategy can help prevent data loss, theft, or corruption and can help minimise damage caused in the event of a breach or disaster (Cloudian, 2023). The key principles of data protection are to safeguard and make data available under all circumstances. It also ensures that users have the data they need to conduct business even if the data is damaged or lost (SNIA, 2023). Data protection regulations govern how certain data types are collected, transmitted, and used. Personal data includes various types of information, including

names, photos, email addresses, bank account details, IP addresses of personal computers, and biometric data (Cloudian, 2023). In terms of data, controllers must clearly disclose any data collection, declare the lawful basis and purpose for data processing, and state how long data is being retained and whether it is being shared with any third parties or outside of the data protection regulation. Also, users should have certain rights over data about them, including the ability to obtain and correct erroneous data about them, and to have mechanisms to seek redress to secure these rights (The World Bank, 2023).

3. Data Privacy, Protection and Security in the Digital Environment

In today's digital world, data privacy, protection, and security are important customer concerns. Individuals must be aware of how their data is being utilised and safeguarded as the quantity of personal and sensitive information acquired and kept digitally grows (Tao & Wang, 2023).

Many businesses gather and utilise consumer data for targeted advertising and other reasons, and customers may be unaware of this or have the option to opt out (Ganeshkumar et al., 2022). As a result, it is critical for businesses to be upfront about their data gathering practices and to provide customers with the opportunity to govern their data (Tuan, 2023). Data breaches occur when unauthorized parties gain access to or steal sensitive information.

Customers must also be conscious of the security of their online platforms and services (Moore, 2023), which includes protecting their personal information on social media and other sites and securing online accounts. They should be wary of phishing schemes, use strong passwords, and keep their software and anti-virus software up to date. Customers have the right to view, amend, and remove their personal data. They must understand their rights and how to exercise them. They also have the right to object to the processing of personal data and request that it be destroyed. Concerns about privacy and anonymity on the internet have developed as a result of the computer's capacity to gather and organize massive volumes of data and the ability of Artificial Intelligence (AI) to transmit it globally.

Users value data privacy because they entrust businesses with personal and sensitive information. One important issue for customers is the collection of personal information without their consent. This emphasizes the necessity of businesses obtaining express consent from individuals before collecting, keeping, or processing their personal data, as well as being honest about their data collection practises. According to a Pew Research Centre (2018) poll, 91% of Americans agree or strongly agree that consumers have lost control over how firms gather and utilize personal information. Online consumer privacy is a big concern, demonstrating that IT users are concerned about how privacy is managed in the digital era (Čtvrtník, 2023).

People are particularly concerned about the possibility of data breaches. According to a Ponemon Institute (2018) survey, the typical data breach costs a firm $3.86 million, and consumers are likely to transfer their business elsewhere following a data breach. Customers should be wary of phishing schemes, use strong passwords, and keep their software and anti-virus software up to date. Payment fraud is a serious problem for Internet-based shops, even though Internet security has mostly focused on possible dangers to customers who use credit cards to complete electronic transactions (Wang et al., 2020). Break-ins and technological disruption are just two of the major security threats; there are several additional critical issues that must be addressed.

Customers are concerned about the sharing and selling of personal information without their authorisation (Oh et al., 2021). Customers should likewise be concerned about the security of their online platforms and services. According to a study conducted by the Centre for Internet Security (CIS), 60% of small firms faced a cyberattack in 2018, and these assaults are growing more sophisticated (CIS, 2018).

According to the United Nations, we live in a digital age. (United Nations, 2013). The advent of technological infrastructure and digital platforms has given rise to surveillance capitalism, which makes use of extensive consumer profiles of personal information. Digital data has become such an essential force in reshaping the architecture of our communities and environments that it is impossible to conceive of a single aspect of life in the Global North that has not been affected by datafication in the last decade.

As major platforms have such large user bases, it is easy to determine whether non-users are linked to active social media users and data created by highly linked and monitored surroundings allows one to make unambiguous remarks not just about people who consent to its collection and usage, but also about those who oppose it. The widespread use of datafication allows for conclusions about people who opt out, regardless of how measures like anonymization are used. In a 'data-fed' society, no one is an island since sharing the same time, location, and cultural dimension makes it difficult for an individual to stand out (Cannataci, 2016).

The rise of online shopping has raised concerns about consumer privacy. Consumer privacy refers to the consumer's ability to control the presence of other participants in a market transaction or the transfer of information to a nonparticipant. This definition, established before e-commerce became prevalent, remains relevant in today's e-commerce environment. Prior to the internet, consumer privacy concerns focused on companies extracting information to target catalogs and promotional messages. However, the rise of the "Age of Information" has heightened the debate on data privacy, as the dynamic nature of web-based technologies has made it a contentious ethical issue. Ireland has a wide legal framework for privacy and data protection, specifically the GDPR and ePrivacy Regulations, which apply to internet consumers.

4. Regulatory Frameworks and the Ghanaian Context

Privacy regulatory frameworks or rules strive to ensure fairness, trust, and responsibility in consumer-firm data transfers. Major privacy frameworks, like other consumer-focused public policies, seek to increase general society well-being and safeguard people's rights while balancing conflicting societal goals such as company profitability and economic growth (Davis et al., 2021; Kopalle & Lehmann, 2021).

The General Data Protection Regulation (GDPR) is a crucial privacy and protection legislation in the world, established by the European Parliament and Council of the European Union on April 14th, 2016, to repeal the Data Protection Directive 95/46/EC. It took effect on May 25th, 2018 and is the major law regulating the conduct of companies and businesses within or outside the EU in protecting the personal information of EU citizens and residents regarding the processing and free movement of such data. This regulation applies to all member states of the European Union to create a uniform data protection law among EU countries. (Alafaa, 2022)

Companies with a digital or physical presence that collect or process personal data of EU residents and citizens are mandated to comply with the GDPR, and failure to comply with this regulation attracts strict penalties and fines. The GDPR became a model for several national laws on data privacy and security across the world. Article 8(3) of the EU Charter of Fundamental Rights explicitly enshrines data privacy and protection as two rights explicitly enshrined in the Charter (Alafaa, 2022). The GDPR comprises 11 chapters, 99 articles, and 173 recitals relating to general privacy principles, rights of data subjects, duties of data controllers, transfer of users' data, liabilities and remedies for breach of rights, and other miscellaneous provisions. It does not apply to the processing of personal information for law enforcement or national security activities of EU member states, and where data is processed for personal or household activities (Alafaa, 2022).

The African Union (AU) has made great progress towards the establishment of a Continental Free Trade Area (CFTA) to encourage the free movement of people, products, and services. This has ramifications for cross-border data transfer, notably in online transactions and for persons who live and work in member states other than their home country. AU member states (for example, Botswana, Democratic Republic of Congo, Egypt, Ghana, Kenya, Nigeria, Sierra Leone, South Africa, Tanzania, Uganda, Zambia and Zimbabwe recognise the right to individual privacy in their national constitutions as a fundamental human right) are also obligated to respect, preserve, and promote the right to privacy and personal data protection, which is recognised in certain nations as a basic human right. These regulations and requirements have ramifications for the secure, transparent, resilient, and privacy-compliant sharing of personal data across borders and countries. This burden on AU member countries is intended to guarantee that progress towards regional integration, free trade, and growth is not hampered or made more difficult.

Ghana, a member of the African Union, Commonwealth Countries, and the Economic Community of West African States, is a signatory to the African Continental Free Trade Agreement (AfCFTA). The country has a policy promoting Information and Communications Technology, the Ghana ICT4AD Policy, which is currently under review. Ghana is expected to launch its Digital Economy Policy, which will replace the Ghana ICT4AD Policy. The country recognises the need for a legal framework to ensure data subject privacy rights are not violated in technology use. (Ghana - Data protection overview, 2023).

The Data Protection Act 2012 is an act to create a Data Protection Commission, to safeguard the privacy of the individual and personal data by regulating the processing of personal information, to provide the procedure to collect, keep, use or disclose personal information and for connected purposes. The date of enactment in Ghana was May 10, 2012. It was passed by the House of Parliament and approved by the President. (Data Protection Act, 2012).

The Data Protection Act, 2012 is a piece of legislation enacted by the Parliament of the Republic of Ghana to protect the privacy and personal data of

individuals. The Act regulates the process by which personal information is acquired, kept, used or disclosed by data controllers and data processors by requiring compliance with certain data protection principles. The key features of the Data Protection Act of Ghana include:

The Act, which outlines what constitutes lawful processing, exempt processing, the scope and duties of data controllers, data processors, the Data Protection Commission, and the rights of data subjects (Codjoe, 2023)

The Data Protection Act of Ghana is like other data protection laws around the world, such as the General Data Protection Regulation (GDPR) in the European Union. Both laws aim to protect the privacy and personal data of individuals and require compliance with certain data protection principles. Thus, it is one of many data protection laws around the world. Some of the ways it compares to data protection laws in other countries are as follows:

5. Challenges to Data Privacy and Protection

In our increasingly interconnected and data-driven world, the challenges encountered in data privacy and protection have become paramount. The exponential growth in data generation and the proliferation of digital technologies have created a complex landscape where safeguarding sensitive information is more critical than ever before. Data privacy and protection regulations have been seen as incredible achievements; yet, there are several issues with the protection of user data. Some of these challenges include:

Extensive data growth

Organisations are required to appropriately secure users' personal information from any sort of data breach, and with the expanding nature and volume of data in our technologically driven society, handling billions of data points becomes burdensome. Also, given the numerous data privacy laws and the complexities of their requirements, there is some scepticism that complete compliance is even conceivable.

Legal entanglement

With the existence of several data privacy and protection laws, the possibility of conflict between several laws can often pose a significant challenge to organisations whose users span multiple continents, affecting their ability to adequately comply with each country's data privacy laws.

Cost of preserving data privacy and security

The expense of repairing a data breach results in a significant loss of revenue for a business, which risks severe regulatory fines. Organisations are obliged to develop and implement suitable measures to guarantee that adequate and specific security technologies, such as data backups and archiving, are in place in order for data to be secured, retrieved, and restored.

Human error

Many data analysts believe that human error is the most major obstacle in data privacy; for example, a lack of understanding among employees can have a substantial impact on an organisation's data privacy and security system. This can happen due to the use of weak passwords, falling for phishing schemes, and other factors, which can expose user data and lead to data loss.

Data breaches and cyberattacks

Data breaches and cyberattacks are perhaps the most immediate and pressing challenges to data privacy. Hackers and cybercriminals relentlessly exploit vulnerabilities in digital systems to gain unauthorised access to sensitive information. The fallout from these breaches includes financial losses, reputational damage, and compromised personal data, affecting both individuals and organisations.

Complex regulatory landscape

The regulatory environment for data privacy and protection is continually evolving. Laws such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the United States have set stringent standards. Compliance with these laws is challenging, as organisations must navigate a patchwork of regulations that vary by region and industry, and non-compliance can result in substantial fines.

Data localisation requirements

Many countries are enacting data localisation laws, requiring organisations to store data within national borders. While these laws aim to protect national security and data sovereignty, they can be challenging for multinational corporations to implement and may result in increased data management costs.

Rapid technological advancements

As technology evolves, so do the methods and tools used by cybercriminals. Emerging technologies such as artificial intelligence, blockchain, and the Internet of Things (IoT) present new challenges for data privacy and protection. Ensuring that these innovations are deployed securely is a constant struggle.

Third-party risk

Organisations often rely on third-party vendors and partners to handle data processing. This introduces a significant risk, as these entities may not have the same level of commitment to data protection,

potentially leading to data breaches or unauthorised access.

Data ethics and consent

Balancing data collection for legitimate purposes with ethical concerns is challenging. Organisations must obtain informed consent from individuals for data processing, and the boundaries of what constitutes "informed" consent can be blurry. Additionally, the ethical implications of data use, such as algorithmic bias, require careful consideration.

Insider threats

While external threats often take centre stage, insider threats from employees or contractors can be equally damaging. Malicious insiders or careless employees can compromise data security, emphasising the need for robust access controls and employee training.

Resource constraints

For smaller organisations and developing countries, resource constraints pose a significant challenge in implementing robust data protection measures. Limited budgets, lack of expertise, and inadequate infrastructure can hinder their ability to safeguard data effectively.

6. Measures for Strengthening Data Privacy and Protection

Organisations operating in multiple jurisdictions must ensure compliance with data privacy regulations such as GDPR, CCPA, and local laws. This involves appointing data protection officers, conducting regular privacy impact assessments, and establishing data protection policies that align with these regulations. Given the rapid pace of technological advancements, organisations should adopt adaptive solutions that harness emerging technologies for data protection. This includes leveraging AI and machine learning algorithms to identify and respond to security threats, as well as exploring the potential of blockchain for data integrity.

Organisations can reduce third-party risks by conducting thorough due diligence on vendors and partners. Contracts should clearly define data protection responsibilities, and regular audits of third-party security practices can ensure compliance. Fostering ethical data practices involves ensuring that data collection is conducted transparently and with informed consent. Organisations should clearly communicate their data usage policies to individuals, and data anonymisation techniques should be employed to protect privacy.

Preventing insider threats requires a combination of technical and organisational measures. Access controls should be stringent, limiting employee access to only the data necessary for their roles. Regular employee training and awareness programs can help mitigate the risks posed by insiders. Smaller organisations and developing countries can access data protection resources and expertise through partnerships and collaborations. Governments can allocate resources to support data security initiatives and provide training and capacity-building programs to raise awareness and improve cybersecurity readiness. To successfully maintain the privacy and security of users' personal data, both organisations collecting and processing the data and users must take relevant and necessary procedures.

6.1. Organisational and User Responsibilities

Organisations have the responsibility of;

1. Raising employee knowledge of the importance of data privacy and security by developing security awareness and training programmes for both existing and new workers, lowering the risk of data loss.
2. Implementation of data loss prevention and security measures to assist in preventing workers or users from leaking sensitive data and lowering the danger of an attack.
3. Ensuring that the organisation's network and systems are consistently monitored in order to spot any suspicious actions or attacks early.
4. Implementation of zero trust models, which would prohibit unauthorised third-party access to the organisation's network.

Users have the responsibility of;

1. Get familiar with privacy technologies such as password managers, which are encrypted virtual private networks that safeguard the user's internet connection. A good password should be lengthy, complicated, and difficult to guess. It is not advisable to use the same password for all user accounts.
2. Scan your device regularly using reliable antivirus software to detect and eliminate any dangerous threats to your device, and back up your data often.
3. Be on the lookout for any unusual requests, flashing clickbait content, or anything that appears to be phoney or suspicious. To avoid such phishing, avoid submitting your personal information on any site that you did not visit, search for, or bookmark on your own.
4. Users are recommended to only disclose their personal information to organisations that are clear and honest about their data privacy rules, do not sell their information for the purpose of amassing enormous rewards, and are not lackadaisical in safeguarding user data.

7. Emerging Trends and Relevance to Ghana

As consumers continue to emphasise data privacy and security, governments are likely to enhance their rules and regulations. This will protect people's privacy and offer corporations clear criteria for securing personal data. Individuals may demand that organisations be more honest about their data practises as they become more aware of data privacy and security, urging enterprises to take more precautions to secure consumer data. Industry collaboration will be critical in finding more effective solutions to keep data private and safe, especially given the increasing frequency of data breaches. As technology advances, new tools, such as blockchain, will most likely be created to aid with data security. This presents a promising future for data privacy and security.

As data privacy concerns continue to grow, there will likely be a greater emphasis on the use of privacy-enhancing technologies such as encryption, anonymisation, and data masking. Data protection regulations are becoming more stringent, and organisations will need to ensure that they are compliant with these regulations to avoid penalties and reputational damage (Bertrand, 2019).

Data protection will continue to be a critical issue for organisations in the coming years, and they will need to stay updated with the latest trends and regulations to ensure that they are adequately protecting their data. In like manner, these trends have significant implications for countries like Ghana, which are also navigating the complex landscape of data security, privacy, and governance. Some of the key future trends in data protection and their relevance to the Ghanaian context include:

Ghana has already made strides in data protection with the passage of the Data Protection Act, 2012 (Act 843). The trend towards more stringent privacy regulations globally will likely encourage Ghana to review and update its existing laws to align with international standards. Ghanaian businesses and government agencies can harness AI and machine learning to enhance data protection measures. Implementing AI-driven security solutions can help identify and mitigate potential threats in real time.

The use of blockchain technology for data security and authentication can benefit various sectors in Ghana, including supply chain management, land registration, and financial services. Implementing blockchain-based solutions can enhance data integrity and reduce the risk of data breaches. With the growing use of biometric data for identification and verification, Ghana needs to establish robust safeguards for the collection and storage of biometric information, especially in areas like national ID systems and financial services.

Ghana should invest in cybersecurity education and training to build a skilled workforce capable of defending against cyber threats. This is vital for protecting critical infrastructure and businesses from data breaches. As cross-border data flows continue to grow, Ghana will need to ensure its data protection laws align with global standards to facilitate international data transfers while safeguarding citizens' privacy. Promoting responsible data governance and ethical use of data is crucial. Ghana can develop guidelines and frameworks to ensure that data is used for the benefit of society while respecting individual rights.

When it comes to its relevance for Ghana, as the Internet of Things (IoT) proliferates, Ghana must address the security challenges associated with connected devices to protect personal data and critical infrastructure. Also, collaborative efforts among government agencies, the private sector, and civil society are essential. Ghana can establish partnerships to share threat intelligence and best practices in data protection.

In summary, the future trends in data protection are highly relevant to Ghana's efforts to safeguard personal data, promote innovation, and foster trust in the digital ecosystem. As the nation continues to develop its digital infrastructure, it must adapt to these evolving trends to ensure the security and privacy of its citizens' data.

8. Conclusion

Data privacy comprises an individual's freedom to freely exist in one's environment without being watched, and data protection is an important means of ensuring that organisations and businesses both comply with the laws and ensure information privacy. Organisations are responsible for preserving users' personal information, and openness by these organisations and enterprises on how user data is acquired, handled, and shared promotes confidence among users. As a result, data privacy and protection strive primarily to safeguard consumers while also ensuring that enterprises and organisations are entrusted with the obligation of preserving users' personal data and are held accountable for any data security breaches.

9. Recommendations

The following recommendations were influenced by the study's results and observations. These guidelines attempt to address the recognised issues and dangers to data protection and privacy that individuals are expected to experience when using the internet.

The need for strong and unique passwords

One of the most important measures in ensuring data privacy is to develop and keep strong, unique passwords for all your online accounts. Avoid using information that is easily guessed, such as birthdays or popular terms. Instead, use complicated combinations of letters, numbers, and symbols. Consider utilising a trustworthy password manager to generate and securely store your passwords. This lessens the possibility of unauthorised access to your accounts and reduces the likelihood of a data breach.

Enable two-factor authentication

This provides an extra layer of protection by forcing you to submit a second form of verification in addition to your password, often something you have, such as a text message or an app-generated code. Even if someone obtains your password, they will still require the second factor to get access to your account. This greatly improves your online privacy.

Update software and applications regularly.

Updating your operating system, application software, and devices is critical for data security. Security patches and upgrades are often released by developers to address vulnerabilities that hackers can exploit. Failure to update your software might expose you to a variety of privacy threats. Set your devices and applications to download and install updates automatically as they become available.

Beware of sharing personal information.

When revealing personal information online, use caution. Oversharing on social media sites should be avoided since hackers may exploit this information for identity theft or social engineering attempts. Be wary of unsolicited requests for personal or financial information, especially if they appear to come from reputable sources. Check the legitimacy of such requests through proper means.

Educate yourself on phishing and scams.

Phishing attacks are a frequent strategy used by hackers to deceive consumers into disclosing personal information. Discover how to spot phishing emails, texts, and websites. Clicking on dodgy websites or downloading files from unknown sources should be avoided. To be aware and preserve your online privacy, educate yourself on the newest frauds and strategies employed by hackers on a regular basis.

References

[1] Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification, in Proceedings of the 5th ACM Conference on Electronic Commerce. doi:10.1145/988772.988777

[2] Austin, L. (2003). Privacy and the question of technology. Law and Philosophy 22, 119–166.

[3] Bertrand, C. (2019). Trends in Modern Data Protection. Enterprise Strategy Group.

[4] Cannataci, J. A. (2016). Human Rights Council Report of the Special Rapporteur on the right to privacy.

[5] Carrascal, J. P. (2013). Your browsing behavior for a big mac: Economics of personal information online, in Proceedings of the 22nd International Conference on World Wide Web. doi:10.1145/2488388.2488406

[6] CaseGuard. (2023). Ghana's Data Protection Act, New Privacy Legislation. From https://caseguard.com/articles/ghanas-data-protection-act-new-privacy-legislation/

[7] CIS. (2018). 2018 Small Business Cyber Security Survey.

[8] Cloudian. (2023). What is Data Protection and Privacy?. From https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/amp/

[9] Codjoe, R. A. (2023). Ghana- data Protection Overview.

[10] Cooley, T. M. (1879). A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract.

[11] Čtvrtník, M. (2023). Personality Rights, Privacy, and Post-mortem Privacy Protection in Archives: International Comparison, Germany and -Protection of Legitimate Interests. In Archives and Records: Privacy, Personality Rights, and Access.

[12] Davis, B. G., & Hamilton, S. (2021). The future of marketing analytics and public policy. Journal of Public Policy & Marketing, 40(4), 447–452.

[13] DeCew, J. (1997). In Pursuit of Privacy: Law, Ethics, and the Rise of Technology. Cornell University Press.

[14] Ganeshkumar, C. D., & Saginala, M. (2023). Application of Drone Technology in Agriculture: A Predictive Forecasting of Pest and Disease Incidence. In Applying Drone Technologies and Robotics for Agricultural Sustainability, pp. 50-81.

[15] Ghana - Data protection overview. (2023). Data Guidance.

[16] Giese, J. J. (2002). Defining Consumer Satisfaction. Academy of Marketing Science Review.

[17] Greenleaf, G. &. (2022). International and regional commitments in Africa data privacy laws: A comparative analysis. Computer Law & Security Review.

[18] H. Jeff Smith, T. D. (2011). T. D. H. X. INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW. MIS Quarterly 35(4), pp. 989-1015.

[19] Harts, C. (2018). Doing a literature review: Releasing the research imagination.

[20] Kopalle, P. K., & Lehmann, D. R. (2021). EXPRESS: Big data, marketing analytics, and public policy: Implications for health care. Journal of Public Policy & Marketing.

[21] Kosinski, M. S. (2013). Private traits and attributes are predictable from digital records of human behavior. doi:10.1073/pnas.1218772110

[22] Leiner, B. &., Cerf, V. &., Clark, D. &., Kahn, R. &., Kleinrock, L. &., Lynch, D. &.,. Wolff, S. (2009). A Brief History of the Internet. Computer Communication Review.

[23] McCombes, s. (2023). How to write a Literature Review | Guide, Examples, & Templates.

[24] Mckenzie, B. (2023). Data Protection Day - Key developments and trends for 2023.

[25] Moore, A. D. (2023). Privacy, Security, and Surveillance. In Technology Ethics , pp. 160-168.

[26] Oh, S. R., & Kim, Y. G. (2021). A comprehensive survey on security and privacy for electronic health data. International Journal of Environmental Research and Public Health, 18(18).

[27] P. (2022). Data privacy and data protection: The right of user's and the responsibility of companies in the digital world. SSRN Electronic Journal.

[28] Pew, P. R. (2018). Americans 'Attitudes about Privacy, Security and Surveillance. 2018 Cost of Data Breach Study: Global Overview.

[29] Revell, T. (2018). How Facebook Let a Friend Pass My Data to Cambridge Analytica. The New Scientist. From https://www.newscientist.com/article/2166435-how-facebook-let-a- friend- pass-my-data-to-cambridge-analytica/

[30] SNIA. (2023). What is Data Protection? From https://www.snia.org/education/what-is-data-protection

[31] Swire, P. P. (2012). Foundations of Information Privacy and Data Protections, Portsmouth. NH: International Association of Privacy Professionals.

[32] Tao, Y. &., & Wang, W. H. (2023). Fair privacy: how college students perceive fair privacy protection in online datasets. Information, Communication & Society, 1-16.

[33] The World Bank. (2023). Data protection and privacy laws. From https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

[34] Tuan, T. N. (2023). Corporate Social Responsibility in Protecting the Right to a Private Life. In Laws on Corporate Social Responsibility and the Developmental Trend in Vietnam, pp. 205-219.

[35] United Nations. (2013). The right to privacy in the digital age. United Nations.

[36] Wang, M. Z., & Zhou, W. (2020). Security and privacy in 6G networks: New areas and new challenges. Digital Communications and Networks, 6(3), pp. 281-291.

[37] Wang, N. &. (2019). Source-location privacy protection based on anonymity cloud in wireless sensor networks. IEEE Transactions on Information Forensics and security,15, 100-114.

[38] Wang, Y. a. (201). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. 246-257.

[39] Warren, S. B. (1890). The right to privacy. Harvard Law Review, 5.

[40] Westin, A. (1967). Privacy and Freedom.

[41] Zou, Y. &. (2018). Concern but no action: consumers' reactions to the equifax data breach," in Proceedings of the Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems.

[42] Zou, Y. a. (2018). Concern but no action: consumers' reactions to the equifax data breach, in Proceedings of the Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems (New York, NY: ACM). doi:10.1145/3170427.3188510