THE SIGNIFICANCE OF DATA PRIVACY IN THE DIGITAL ECONOMY[1]

Senior Research Fellow, Radoslav Baltezarevıć
ORCID: https://orcid.org/0000-0001-7162-3510
radoslav@diplomacy.bg.ac.rs
Institute of International Politics and Economics, Belgrade, Republic of Serbia

Associate Professor, Ivana Baltezarević
ORCID: https://orcid.org/0000-0003-4605-1420
ivana.baltezarevic@gmail.com
Faculty of Law, Megatrend University, Belgrade, Republic of Serbia

Abstract

Protecting our identity, habits, health, interests, and everyday activities is known as data privacy. Data privacy entails protecting personal data and making sure that people have authority over the collection, use, and sharing of their data. Governments, organizations, and individuals are increasingly generating, collecting, and processing personal data. Strong data privacy laws promote consumer confidence and encourage more people to utilize digital tools, which can encourage competition, investment, and innovation in the digital economy. By giving people control over their data and the freedom to engage with the digital world however they choose, data privacy empowers people. Additionally, it helps prevent cybercrimes, including fraud, harassment, and identity theft. Data availability is crucial for start-ups and new enterprises to create new products and services. However, their capacity to compete with well-established market competitors may be disproportionately impacted by overly onerous privacy restrictions. The digital economy depends heavily on user trust and security. A key component of this trust is cybersecurity, which includes safeguards against intrusions, damage, and unauthorized access to digital systems, networks, and data. Real-time cyber threat detection and response are possible with artificial intelligence (AI) and machine learning (ML). These technologies are capable of automatically implementing security measures and identifying possible security breaches by analysing patterns and anomalies in data. Maintaining cybersecurity and privacy is crucial for encouraging digital inclusion and safeguarding communities as the digital economy grows.

Keywords: Data Privacy, Digital Economy, Cybersecurity.

[1] The paper presents findings of a study developed as a part of the research project “Serbia and challenges in international relations in 2024”, financed by the Ministry of Science, Technological Development and Innovation of the Republic of Serbia, and conducted by Institute of International Politics and Economics, Belgrade during year 2024.

INTRODUCTION

Information collection, processing, sharing, and violation are only a few of the many actions that fall under the broad category of privacy (Solove, 2008). Both younger and older consumers seem to be growing increasingly concerned about privacy over time; however, older consumers' concerns seem to be growing more significantly (Goldfarb & Tucker, 2012). Half of the customers polled in an Ernst & Young analysis said they would be less inclined to divulge personal information in the future. This research indicates that businesses are already preparing for less access to consumer-provided data, which makes more subversive data collection techniques appealing (Ernst & Young, 2015). The situation of internet users' online privacy has drastically changed in recent years. We've seen it shift from ignoring certain aspects of online data privacy and unchecked data use by internet businesses to enforcing data safety regulations in businesses and letting users choose how much information they want to give. Nevertheless, more work needs to be done. In order to comply with current privacy rules, organizations still require additional direction. In the same vein, privacy laws must be adapted to the quickly evolving sector (Petrosyan, 2024a).

In 2024, the data security market is expected to generate more than $7 billion in revenue. By 2029, revenue is anticipated to expand at a compound annual growth rate (CAGR) of 11.28%, reaching a market value of more than US$12 billion (Statista Market Insights, 2024). Consumers directly profit economically from data flows in the digital environment. They take advantage of innovative services like recommendation and search engines, tailored offers and advertisements, and focused goods and services. Additionally, customised communication can help clients make well-informed decisions and lessen information overload (Ansari & Mela, 2016). The question of which information sources are reliable is one that users of social media and internet technologies are increasingly asking themselves (Baltezarević & Baltezarević, 2021). The need for privacy and data protection is becoming more widely acknowledged as more and more social and commercial activities take place online. The gathering, use, and disclosure of personal data to third parties without customers' knowledge or consent is equally concerning. Out of 194 nations, 137 have laws in place to provide data and privacy protection (Unctad, 2021).

Data protection aims to strike a balance between the advantages and disadvantages of processing personal data so that people can feel secure knowing that their information is gathered, held, and used only for appropriate purposes. The adoption of digital government and private sector services, as well as investment, competition, and innovation in the digital economy, may be stimulated by a robust data protection framework that offers assurance (UNCDF, 2022). Prices can decrease when businesses gain access to data. Using data from 300,000 Google Play Store apps, for example, Kummer and Schulte demonstrate that paid apps ask for less user

data than free apps. In addition to the financial advantages, customers may directly gain psychologically from data sharing (Kummer & Schulte, 2019). Open data flows provide businesses with additional information to personalize their messages, goods, and services for each unique customer. Personalization can help consumers make more informed decisions by reducing information overload. Allowing businesses to understand their preferences lowers customer search expenses for consumers, enabling the right messages and products to reach the right person at the right time (Goldfarb & Tucker, 2019). Businesses gain from targeted advertising made possible by data flows. By using targeting, the company may prevent wasteful advertising and naturally boost market distinction (Iyer et al., 2005).

Growing advances in privacy-preserving machine learning (ML) systems allow for the protection of consumer privacy while yet allowing for the extraction of useful data to enhance products and services (Zhou et al., 2020). New methods of information processing are made possible for businesses by developments in network and communication technology. However, these recent advancements in the processing of personal data could affect a person's daily life and introduce new concerns like: transparency (the intricacy of emerging technologies may result in unclear and opaque personal data processing); loss of control (people's comprehension of the systems that handle their personal data may be limited due to the quick growth of technology, which may ultimately limit their ability to exercise control over such data); manipulation (more focused advertising is now possible because of digitalization). Certain weaknesses may be exploited by targeted advertising, which could result in manipulation and compromise personal freedom and autonomy) (GRA, 2022).

LITERATURE REVIEW

According to Nissenbaum, privacy is the authority to control the flow of personal data (Nissenbaum, 2009). Over the years, a number of privacy issue metrics have been developed and examined with a range of causes and consequences. A reliable indicator of people's self-reported privacy concerns covers the following topics: data acquisition; improper access; illegal secondary usage; and error protection (Smith et al., 1996). According to a 2023 survey, nearly 40% of consumers globally think that a company may gain customers' trust by being transparent about how it uses their data. Another 24% of respondents stated that if companies refrain from selling customer data, they may gain greater credibility, and more than 20% stated that it is crucial to adhere to all privacy laws (Petrosyan, 2024b).

One effective method of getting to know clients is behavioral profiling, which is based on both in-person and online purchase habits. One could argue that being watched in some way is neither unusual nor shocking when it comes to e-commerce or retail shopping. Through increasing capabilities to synthesize data from places

where customers might not expect marketers to be, data aggregating tools have enabled marketers to push the limits of organic customer observation. Irrelevant social media searches on topics such as health issues, consumer vehicles, and televisions and cell phones can provide information for these insights (Kshetri, 2014). Companies' irresponsibility in protecting the data of their customers might harm and compromise their reputation (Baltezarević & Baltezarević, 2022). Apple's recent decision to deny U.S. law enforcement backdoor access to a known terrorist's iPhone has made protecting consumer privacy a major topic of discussion in both social and professional circles. In fact, the debate's headlines addressed the idea of utilizing privacy as a tactic explicitly by quoting government prosecutors who said that Apple's rejection was motivated by its concern for its public brand marketing strategy. The company's refusal is marketing-related in the sense that they are concerned with preserving consumer information, property, and privacy, all of which they know their customers value (Lichtblau & Apuzzo, 2016).

Privacy policies can serve as a useful stand-in for how much more power and transparency businesses give their clients, connecting such aspects to business performance and customer behavior. A company with a strong privacy policy can protect itself from possible negative consequences resulting from a close competitor's privacy lapse. Combining this with the broader trend of businesses self-regulating their privacy practices with consumer information indicates that having a clear and concise privacy policy is crucial (Martin et al., 2017). A complex system, the General Data Protection Regulation (GDPR) law of the European Union requires websites to acquire consent for data tracking, give users a number of rights over the use of their data, and mandate specific storage and security criteria. The regulation may not have succeeded in increasing user privacy, but it has created a number of new issues (Purnell, 2023).

Businesses can better understand their clients' demands by using data. Granular activity data from customers can help businesses adopt proactive retention tactics. Consumer data, for instance, may indicate that users of subscription services are at risk of terminating their memberships. The marginal effects of various client retention initiatives can also be seen in these data (Ascarza, 2018). Businesses must prioritize protecting the privacy of their customers' data. To become a leader in its sector, a company must not only be able to adapt but also anticipate all changes and trends in the near future (Baltezarević & Baltezarević, 2019). According to Taylor, the degree of knowledge of customers determines how beneficial privacy regulations are when tracking technologies are in place, enabling retailers to determine customer preferences and discriminate on price. Unless privacy protection is enforced by regulation, corporations will capture their surplus since naive consumers do not expect a seller to utilize every detail about their previous contacts for price discrimination. However, if customers are aware of how merchants may use their data and modify their behavior accordingly, regulation is

not required because it is in a company's best interest to secure customers' data, even in the absence of an explicit rule requiring it to do so (Taylor, 2004). A low-quality company may decide to disclose consumer data in response to competitive pressure if there is a data market. The existence of an extra money stream from data sales undermines the incentives for quality improvement when businesses have two revenue streams: the disclosure revenue from selling consumer data and the sales revenue from products. Consumer data helps organizations focus on differentiating their privacy practices and reduces the intensity of competition when consumers are diverse (Casadesus-Masanell & Hervas-Drane, 2015).

Campbell and colleagues showed that the entrenchment of monopolies might be an unforeseen effect if privacy legislation solely depended on ensuring opt-in consent. The authors demonstrate that consumers are more inclined to give their opt-in agreement to extensive, big networks than to smaller, less well-known businesses. Users may be less inclined to check out services from newer companies and entrants if the law just concentrates on enforcing an opt-in approach. This could result in a natural monopoly, where scale economics includes privacy protection, and hence create obstacles to entry (Campbell et al., 2003). Data collection and safe storage are expensive. Businesses must contend with difficult legal requirements and compliance standards. They must make expensive investments to safeguard stored customer data against nefarious third-party access, including cyberattacks. Updates to the application programming interface (API), enhanced firewalls, and vulnerability assessments by hackers employed by the firm are ways that data is protected. In comparison to this expense, the advantages of data might be minimal (Shy & Stenbacka, 2016).

Artificial intelligence (AI) is being used more and more in a variety of security domains to improve cybersecurity, incident response, and threat identification. By strengthening threat detection, response capabilities, and general cybersecurity measures, AI raises security (Hewlett Packard Enterprise, 2024). Nevertheless, it is not advised to rely solely on technology during the digital transformation process (Papakonstantinidis et al., 2021). On the other hand, the kinds of personal data that AI systems can gather are growing quickly as they get more sophisticated and integrated into our daily lives. We may not even be aware of the amount of information AI systems are collecting about you throughout the course of your day. AI systems gather and analyze vast amounts of data, including location data, web activity, voice and facial recognition, and personal information. Despite its many applications, artificial intelligence poses a number of privacy dangers and challenges (Granados, 2024). Unchecked AI has the potential to distribute modified content, including deepfake videos, reinforce biases, and amplify toxic content. Misinformation, discrimination, and harm to people and society may result from this (Granados, 2024).

Even though empirical research is still in its infancy, recent developments at Google and Apple should contribute to a deeper comprehension of business motivations for privacy preservation. In particular, Google and Apple have limited the kinds of data flows that can leave their operating systems and devices and reach other parties (Bergen, 2021). A significant amount of engineering work has been done to limit the flow of personally identifiable data while facilitating data-driven innovation. Using so-called differential privacy, which attempts to ensure that data can be utilized for statistical analysis while maintaining anonymity, is one development (Abowd & Schmutte, 2019).

CONCLUSION

Considering the possible risks associated with the digital economy, in addition to the advantages of using digital tools, the significance of data privacy becomes even more clear. In this sense, data protection aids in establishing and preserving credibility. Data security laws offer protections that uphold people's rights and liberties regarding their personal information while also fostering the growth of the digital economy.

Protecting cybersecurity and privacy requires strong legislative and regulatory frameworks. Laws protecting personal information and requiring digital service providers to follow strict security guidelines should be passed and enforced by governments. One excellent example of comprehensive data protection law that might serve as an inspiration for comparable frameworks around the world is the General Data Protection Regulation (GDPR) of the European Union. The Personal Data Protection Bill is an attempt to create a legislative framework for privacy and data protection with the goal of safeguarding citizens' private information and regulating data management procedures.

Protecting personal information from artificial intelligence (AI) privacy issues should ultimately be a primary concern for businesses nowadays. As AI applications proliferate, it is imperative that businesses take the appropriate precautions to safeguard user data if they hope to stay competitive in the digital future. However, by restricting access to data and impeding its smooth movement between industries and organizations, stringent data privacy laws can stifle innovation. Therefore, maintaining a dynamic, competitive marketplace requires finding a balance between protecting people's privacy and creating an atmosphere that encourages innovation.

LITERATURE

Abowd, J.M. & Schmutte, I.M. (2019). An economic analysis of privacy protection and statistical accuracy as social choices. Am. Econ. Rev. 109(1):171–202.

Ansari, A. & Mela, C.F. (2016). E-customization. J. Mark. Res. 40(2):131–145.

Ascarza, E. (2018). Retention futility: Targeting high-risk customers might be ineffective. J. Mark. Res. 55(1):80–98.

Baltezarević, I. & Baltezarević, R. (2019). Prikriveno oglašavanje u novim medijima, Baština, sv. 48, pp. 171-179. UDK 659.1 doi: 10.5937/bastina1948171B

Baltezarević, I. & Baltezarević, R. (2021). Sajber bezbednost: izgradnja digitalnog poverenja, Megatrend Revija, Vol. 18 (4), 269-280. doi: 10.5937/MegRev2104269B

Baltezarević, R. & Baltezarević, V. (2022). The influence of digital political communication supported by neuromarketing methods on consumer perception towards a tourist destination. *Megatrend revija,* Vol. 19, No 2, 13-34. doi: 10.5937/MegRev2202013B

Bergen, M. (2021). Apple and Google are killing the (ad) cookie. Here's why. Retrieved from: https://www.bloomberg.com/news/articles/2021-04-26/how-apple-google-are-killing-the-advertising-cookie-quicktake#xj4y7vzkg (Accessed: 13.11.2024.)

Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. Journal of Computer Security 11 (3), 431–448.

Casadesus-Masanell, R. & Hervas-Drane, A. (2015). Competing with privacy. Manag. Sci. 61(1):229–246.

Ernst & Young (2015). Megatrends 2015: Making sense of a world in motion. EY Global Report.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. American Economic Review, 102, 349–353.

Goldfarb, A. & Tucker, C. (2019). Digital economics. J. Econ. Lit. 57(1): 3–43.

GRA (2022). The importance of data protection for the digital economy. Retrieved from: https://www.gra.gi/uploads/documents/data-protection/Privacy%20Awareness/Social%20Media%20Campaigns/The%20Digital%20Economy%20-%20Infographics.pdf (Accessed: 14.11.2024.)

Granados, A. (2024). AI and Personal Data: Balancing Convenience and Privacy Risks. Retrieved from: https://velaro.com/blog/the-privacy-paradox-of-ai-emerging-challenges-on-personal-data (Accessed: 13.11.2024.)

Hewlett Packard Enterprise (2024). What is AI Security? Retrieved from: https://www.hpe.com/in/en/what-is/ai-security.html (Accessed: 15.11.2024.)

Iyer, G., Soberman, D. & Villas-Boas. J.M. (2005). The targeting of advertising. Mark. Sci. 24(3): 461–476.

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. Telecommunications Policy, 38, 1134–1145.

Kummer, M. & Schulte, P. (2019). When private information settles the bill: money and privacy in Google's market for smartphone applications. Manag. Sci. 65(8):3470–3494.

Lichtblau, E. & Apuzzo, M. (2016). Justice department calls Apple's refusal to unlock iPhone a 'marketing strategy.' New York Times. Retrieved from: https://www.nytimes.com/2016/02/20/business/justice-department-calls-apples-refusal-to-unlock-iphone-a-marketing-strategy.html (Accessed: 15.11.2024.)

Martin, K. D., Borah, A. & Palmatier, R. W. (2017). Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing*, *81*(1), 36-58. https://doi.org/10.1509/jm.15.0497

Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, CA: Stanford Univ. Press.

Papakonstantinidis, S., Kwiatek, P., Baltezarević, R. (2021). The impact of relationship quality and self-service technology on company performance. *Polish Journal of Management Studies 2021*; 23 (1): 315-326.

Petrosyan, A. (2024a). Online privacy worldwide - Statistics & Facts. Retrieved from: https://www.statista.com/topics/8002/online-privacy-worldwide/ (Accessed: 14.11.2024.)

Petrosyan, A. (2024b). Global consumers on data privacy priorities effective to build trust 2023. Retrieved from: https://www.statista.com/statistics/1369919/consumers-data-privacy-building-trust-global/ (Accessed: 14.11.2024.)

Purnell, S. (2023). The Economics of Data Privacy The Economics of Data Privacy. Retrieved from: https://thedailyeconomy.org/article/the-economics-of-data-privacy/ (Accessed: 14.11.2024.)

Shy, O. & Stenbacka, R. (2016). Customer privacy and competition. J. Econ. Manag. Strategy 25(3):539–562.

Solove, D.J. (2008). Understanding Privacy. Cambridge, MA: Harvard Univ. Press.

Smith, J. H., Milberg, S. J., & Burke, J. B. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 167–196.

Statista Market Insights (2024). Data Security - Worldwide. Retrieved from: https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/data-security/worldwide (Accessed: 15.11.2024.)

Taylor, C. R. (2004). Consumer privacy and the market for customer information. RAND Journal of Economics 35 (4), 631–650.

UNCDF (2022). The role of data protection in the digital economy. Retrieved from: https://policyaccelerator.uncdf.org/all/brief-data-protection-digital-economy (Accessed: 14.11.2024.)

Unctad (2021). Data Protection and Privacy Legislation Worldwide. Retrieved from: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Accessed: 14.11.2024.)

Zhou, Y., Lu, S. & Ding, M. (2020). Contour-as-face framework: a method to preserve privacy and perception. J. Mark. Res. 57(4):617–639.