Privacy in computer ethics: Navigating the digital age

Maxwell Zostant, Robin Chataut
Department of Computer Science, Fitchburg State University, Fitchburg, MA, 01420, USA

Article Info

Article history:

Received Apr 15, 2023
Revised Jun 4, 2023
Accepted Jun 20, 2023

Keywords:

Encryption
Ethics
Privacy
Protection
Security

ABSTRACT

In this digital age, privacy has become a crucial issue due to the vast amount of personal information we share online. As a fundamental aspect of computer ethics, it concerns the appropriate use of information and communication technologies. This paper will discuss five key points related to privacy in computer ethics: the concept of privacy and its significance in the context of computer ethics; ethical considerations surrounding personal information in the digital space, including issues of consent, transparency, and data protection; the legal framework surrounding privacy in different jurisdictions, such as data protection laws and international standards; the role of technology in protecting privacy, including the use of encryption and other security measures; and finally, the challenges associated with protecting privacy in the digital age, such as the risk of data breaches, identity theft, and other forms of online exploitation. Through these five key points, this paper aims to provide a comprehensive understanding of privacy in computer ethics and emphasize the importance of promoting responsible and ethical use of technology.

Corresponding Author:

Robin Chataut
Department of Computer Science, Faculty of Computer Science, Fitchburg State University
160 Pearl St, Fitchburg, Massachusetts, 01420, USA
Email: rchataut@fithcburgstate.edu

1. INTRODUCTION

Privacy is a fundamental human right that is vital in the context of computer ethics. Privacy refers to the ability of individuals to control their personal information and to prevent unwanted intrusion or exploitation. In the digital age, privacy has become a critical issue due to the vast amount of personal information that is being collected, stored, and analyzed by organizations around the world. As a result, computer ethics has developed a range of ethical principles and guidelines to ensure that individuals' privacy rights are respected.

The concept of privacy has existed since the inception of computer technologies. Around the 1960s, concerns about the potential misuse of personal data by large corporations and government agencies began to emerge. As a result, the government responded by developing strict privacy laws that discouraged acts of privacy violation. One such law was the U.S. Privacy Act of 1974, which regulates the assembly, use, and dissemination of personal data by federal agencies [1]. However, with the massive growth of internet technology in the 1980s, the threat of computer privacy became eminent once more due to the development of technologies such as cookies, web beacons, and tracking software, which made it easy for corporations to steal people's personal data [2], [3]. To enhance personal privacy, technologies like encryption, pseudonymization, and anonymization were developed to counter the threat to computer privacy. Nonetheless, the 21st century saw an amplification of computer privacy concerns because of the increase in social media use. Big tech giants like Google and Facebook have continually violated privacy concerns which has led to public outrage and a spike in computer privacy concerns [4].

Privacy is a multifaceted and intricate concept in computer ethics. Several scholars have researched this topic to gain an understanding of various issues related to the concept. In 2019, the University of Pennsylvania conducted a study on computer privacy and noted that a staggering 91% of computer consumers in the United States believed that they didn't have autonomy over their personal data. In addition, the study found that approximately 84% of Americans have concerns about their personal data on major web browsers and social media platforms. According to the study, many U.S. citizens believe that technology has become pervasive in their daily lives [5]. A similar study by the Pew Research Center in 2019 also indicated that approximately 62% of all American adults perceived that larger corporations, like Google and Facebook, posted a threat to their personal data shown is Figure 1 [6].

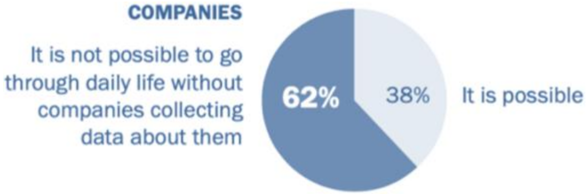

Figure 1. 62% of American citizens believe that it is not possible to use technological devices without companies collecting personal data

Additionally, a separate study conducted by the Ponemon Institute in 2020 indicated that data breaches cost U.S. organizations an average of 4.24 million per breach. Even worse, the healthcare system in the U.S. experienced the highest cost per breach, at $499 per record [7]. Similar research was conducted by the European Union Agency for Fundamental Rights (FRA) in 2019, indicating that 86% of all Europeans felt they didn't have autonomy over their personal data. In addition, around 60% of Europeans showed concerns about not knowing what happens to their personal data once it has been stolen. Concisely, these studies help to highlight the growing concerns about personal privacy in the digital age [8]. Succinctly, these studies also highlight the financial implications that privacy violation has resulted to people and organizations, especially in the United States.

2. IMPORTANCE OF PRIVACY IN COMPUTER ETHICS

Privacy is important in the context of computer ethics for several reasons. Firstly, privacy is essential to the autonomy and the dignity of individuals. The ability to control one's personal information is a fundamental aspect of human autonomy and enables individuals to make informed decisions. A study from the Pew Research Center (PRC) indicates that approximately 74% of adults in the U.S. perceive that it is crucial to control who can have access to their personal data [8]. Concisely, without data autonomy, individuals are at risk of discrimination which may limit their ability to express themselves freely and to participate fully in society. Additionally, privacy is crucial to protecting individuals from harm. Within today's digital age, personal information is increasingly being used to target individuals for various forms of exploitation, such as identity theft, fraud, and harassment [9]. A study conducted by the Norton LifeLock indicated that in the year 2020, around 20% of adults in the United States were victims of identity theft, with financial losses totaling $17 billion [10]. To ensure individuals' privacy rights are respected, computer ethics can help to prevent different forms of harm and promote a safe and secure digital environment. To ensure that everyone's privacy is protected in the digital space, computer ethics has developed several ethical principles and guidelines. One of the key principles is informed consent, which holds that individuals should have the right to control how their personal information is collected, used, and shared. They would also be fully informed about the purpose for which their information is being collected and the potential risks associated with sharing it. Informed consent is particularly important in situations where individuals are asked to provide sensitive personal information; where a few examples are medical information or financial data. In some cases, individuals may not fully understand the potential risks associated with sharing their information and may be vulnerable to exploitation or abuse. Degeling *et al.*, 2019 in their study found that only 40% of all the websites meet the minimum criteria for informed consent [11], meaning that many corporations and organizations are not adequately informing their consumers about their data collection practices. However, to mitigate this concerning issue, the General Data Protection Regulation demands that corporations obtain explicit informed consent from their consumers prior to collecting personal information. Figure 2 shows average costs of a data breach broken down by industry, with average costs totaling.

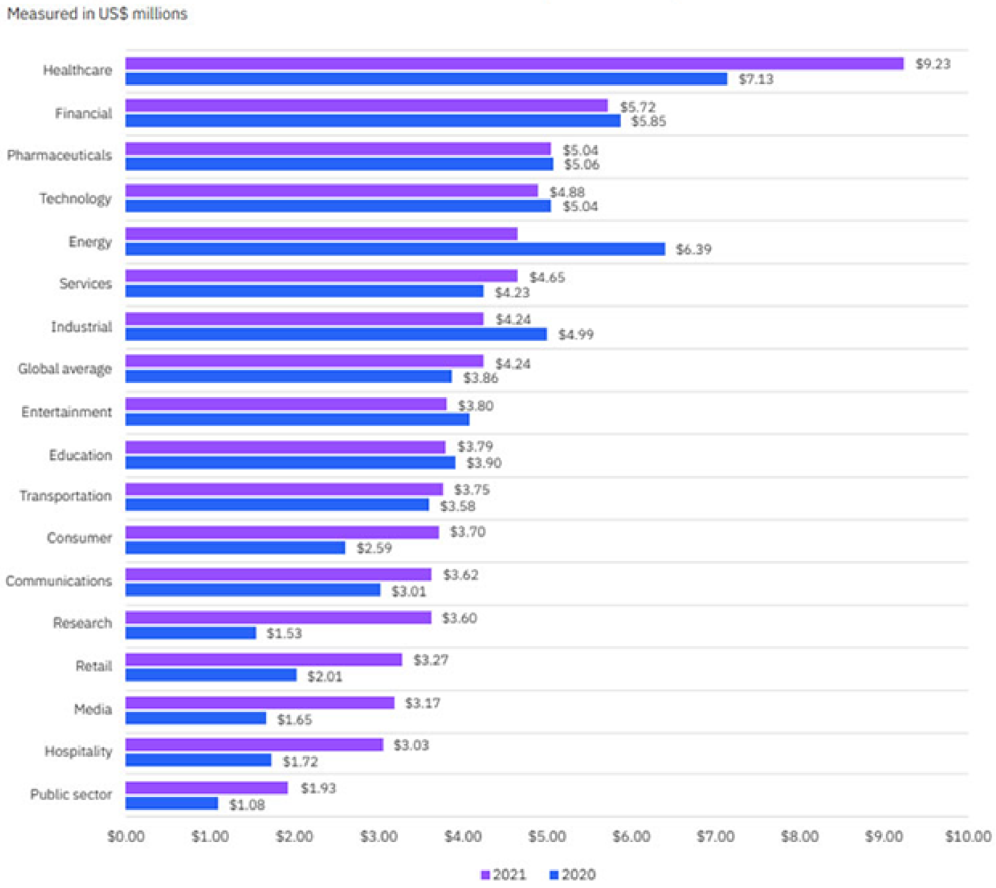

Figure 2. Average costs of a data breach broken down by industry, with average costs totaling

Another important principle of computer ethics is data minimization. This holds that organizations should only collect and retain the minimum amount of personal data necessary to achieve their objectives. This helps limit the potential risks associated with data breaches and identity theft. Data minimization also reduces the potential for organizations to misuse personal information for commercial or other purposes [12]. Figure 3 shows raising concerns of identity theft and fraud complaints between 2018-2022.

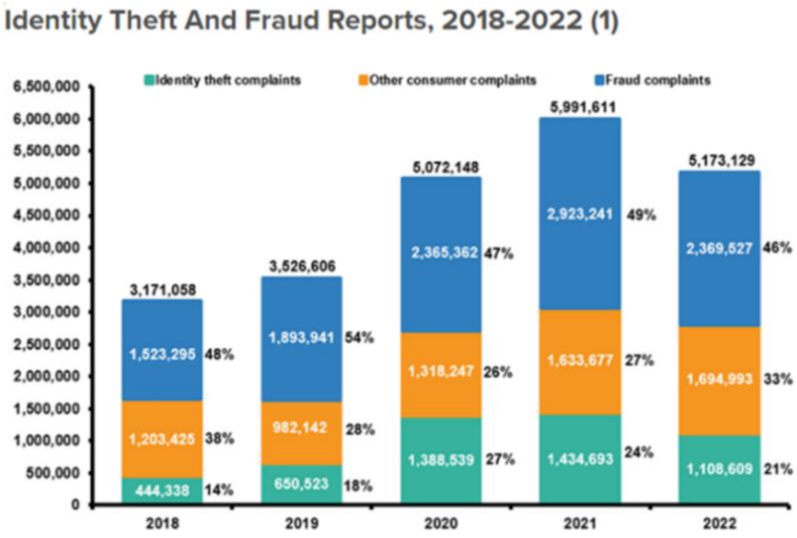

Figure 3. Raising concerns of identity theft and fraud complaints between 2018-2022

3. ETHICAL CONSIDERATIONS DEALING WITH PERSONAL INFORMATION IN THE DIGITAL SPACE

When dealing with personal information in digital spaces, there are several ethical considerations that must be considered. These considerations revolve around issues of consent, transparency, and data protection. This widespread collection and use of personal data by companies and organizations have raised concerns about the potential misuse and exploitation of this information and has led to the development of ethical guidelines and principles to ensure that individuals' privacy rights are respected.

One of the most important ethical considerations when dealing with personal information in digital spaces is the issue of consent. Informed consent requires that individuals be fully informed about the purposes for which their personal data is being collected and used. They have the right to control how their personal data is used. They have the right to control how their personal data is used. Consent is particularly important when dealing with sensitive personal data [13]. Transparency is another key ethical consideration when dealing with sensitive personal data in the digital space. Transparency requires that companies and organizations be open and also honest about their data collection and use practices and that they provide individuals with clear and accessible information about how their data is being used [14]. This includes providing individuals with clear and concise privacy policies and ensuring that individuals have the ability to access and correct their personal data if it is necessary.

Data protection is another important ethical consideration when dealing with personal data in the digital space [15]. Data protection requires that companies and organizations take appropriate measures to safeguard personal data from unauthorized access, use, or disclosure. This includes implementing strong security measures, such as encryption and firewalls, and ensuring that employees are trained to handle personal data in a responsible and ethical manner [16]. The overall ethical considerations surrounding personal information in the digital space are complex. To ensure that individual privacy rights are respected, it is essential that companies and organizations adopt a proactive approach to data protection and transparency. They make a concerted effort to obtain informed consent from individuals before collecting and using their personal data [17].

One example of an ethical framework for dealing with personal information in the digital space is the European Union's General Data Protection Regulation which is also known as GDPR. GDPR is a comprehensive data protection law that sets out clear guidelines and principles for the collection, use, and storage of personal data [18]. The GDPR requires companies to obtain informed consent from individuals before collecting and using their personal data. This provides individuals with clear and concise information about how their data is being used.

Another example of an ethical framework for dealing with personal data in the digital space is the Fair Information Practice Principles which are also known as FIPPs. The FIPPs are a set of guidelines developed by the US government that outline the key ethical considerations for the collection, use, and storage of personal data [19]. The FIPPs require that individuals be informed about the purposes for which their personal data is being collected and used and that they have the right to control their personal data being used.

4. LEGAL FRAMEWORK SURROUNDING PRIVACY IN DIFFERENT JURDICTIONS

The third important ethical consideration when dealing with personal information in digital spaces is the potential for discrimination and bias in data collection and analysis [20]. In recent years, concerns have arisen about the ways in which personal data can be used to perpetuate or exacerbate data collection and analysis and to develop strategies for addressing potential biases and discriminatory practices. One of the main ways in which bias and discrimination can enter into data collection and analysis is through the use of algorithms and automated decision-making systems. These systems rely on data inputs to generate predictions or recommendations, and as such, the quality and accuracy of these outputs depend heavily on the quality and accuracy of the data inputs. If the data inputs are biased or incomplete, then the outputs of the system are likely to be biased as well. An example is the use of predictive policing algorithms, which use historical crime data to predict future crime hotspots and allocate police resources accordingly. However, research has shown that these algorithms are often biased against minority communities, as they are based on historical data that reflect biased policing practices and racial profiling [21].

To address these issues, it is important to adopt a proactive approach to addressing potential biases and discriminatory practices in data collection and analysis. This may involve developing more representative and diverse data sets, as well as ensuring that decision-making algorithms are regularly audited and tested for potential biases. Additionally, it is important to promote transparency and accountability in the use of these systems and to ensure that individuals are aware of how their personal data is being used and analyzed.

One example of the ethical framework for addressing bias and discrimination in data collection and analysis is the concept of "data justice." Data justice is a framework that seeks to promote social justice in the use of data by ensuring that the collection, analysis, and dissemination of data is fair, transparent, and accountable [22]. Data justice advocates for greater public involvement in decision-making around data collection and analysis, as well as greater scrutiny of automated decision-making systems to ensure that they are not perpetuating existing social inequalities and biases. Another example of an ethical framework for addressing bias and discrimination in data collection and analysis is "fairness, accountability, and transparency," which is otherwise known as the FAT approach. The FAT approach seeks to promote the ethical and responsible use of algorithms and automated decision-making systems by ensuring that they are designed and deployed in ways that are fair, transparent, and accountable. The FAT approach emphasizes the need for ongoing testing and auditing of these systems, as well as greater public engagement in decision-making around their use.

5. ROLE OF TECHNOLOGY IN PROTECTING PRIVACY

The fourth ethical consideration when dealing with personal information in digital spaces is the issue of informed consent. Informed consent is the principle that individuals should have the right to make informed decisions about how their personal information is collected, used, and shared. In the context of digital spaces, informed consent is particularly important, as personal data is often collected and used without individuals' knowledge or explicit consent.

One of the main challenges with informed consent in digital spaces is the complexity and opacity of data collection and analysis processes. Many individuals are concerned about the extent to which their personal data is being used and may not trust that organizations or corporations will handle their data while adhering to computer ethics [23]. The prevalence of the general public's distrust towards those who handle their data can make it difficult to promote overall transparency and culpability around information collection and analysis practices. To address this challenge, it is crucial for organizations to enhance transparency in their data collection and analysis practices in order to gain the trust of individuals. This could include measures such as the use of independent third-party auditors to verify compliance with privacy regulations and also regular audits of data practices.

Additionally, another challenge with promoting informed consent in digital spaces is the legal and technical language used in privacy policies and terms of service agreements. Concisely, organizations often employ language with uncommon terminologies which may not be understood by many people. The use of such terminologies may lead to people giving consent about the use of their personal information unintentionally, leading to extreme violations of privacy rights to innocent individuals. To mitigate this issue, the language used in terms of service should be clear and simple to ensure that all people, regardless of their educational backgrounds, have a clear understanding of the terms of service that they are consenting to.

Another challenge with promoting informed consent in digital spaces is that, even when individuals are aware of the collection and use of their personal data, they may not have the ability to make informed decisions about how this data is used. In many cases, individuals may be required to agree to data collection and analysis practices in order to use certain services or access certain information [17]. This creates a situation in which individuals may feel that they have no choice but to agree to these practices, even if they do not fully understand or agree with them. To address this issue, regulations should be in place to ensure that all decisions regarding privacy consent are on the consumer. Organizations must not acquire personal information from individuals who do not want to offer their personal information or data.

Overall, it is essential to promote greater transparency and clarity around data collection and analysis practices. This may involve simplifying privacy policies and terms of service agreements, as well as providing individuals with more accessible and understandable information about how their personal data is being used. Additionally, it is important to provide individuals with greater control over their personal data by giving them the ability to opt out of certain data collection and analysis practices or to request that their data be deleted. An example of an ethical framework for promoting information consent in digital spaces is the concept of "data autonomy." Data autonomy is a framework that seeks to promote individuals' right to make informed decisions about how their personal data is collected, used, and shared. Data autonomy emphasizes the need for individuals to have greater control over their personal data, as well as greater transparency and accountability from companies and organizations that collect and use this data. Another example of an ethical framework for promoting informed consent in digital spaces is the concept of "data sovereignty." Data sovereignty is a framework that seeks to promote individuals' right to control their personal data by giving them ownership and control over this data. Data sovereignty emphasizes the need for individuals to have greater control over the use and sharing of their personal data as well as greater transparency and accountability from companies and organizations that collect and use this data. Concisely, adhering to these ethical frameworks will aid in promoting information autonomy and consequently reduce data violation concerns.

6. CHALLENGES ASSOCIATED WITH PROTECTING PRIVACY IN THE DIGITAL AGE

The fifth ethical consideration when dealing with personal information in digital spaces is the issue of data security. Data security refers to the measures that companies and organizations take to protect personal information from unauthorized access, use, or disclosure. Data breaches and other forms of cyber-attacks can have significant consequences for individuals, including identity theft, financial fraud, and reputational damage [6]. In addition to these harms, data breaches can also undermine trust in the institutions and organizations that collect and use personal information.

One of the main challenges with data security in digital spaces is the constantly evolving nature of cyber threats. Cyber threats refer to any malicious activities that aim to compromise or damage digital systems, networks, or devices. The challenge arises because hackers and other malicious actors are constantly developing new methods and strategies for gaining unauthorized access to personal data, making it extremely difficult for companies to keep up with them [24]. Additionally, the pace at which cyber threats evolve is incredibly fast. Concisely, a security measure that is hack-proof today may not be effective against cyber threats tomorrow.

Another challenge that is associated with protecting privacy in the digital age is that companies and organizations collect and store vast amounts of personal data. The problem arises because the more personal information an organization collects, the more it must be protected [25]. Managing such vast amounts of data is a daunting task, especially with the wide range of ways in which this data can be stored and shared across various platforms, devices, and systems. Additionally, some companies rely on third-party vendors and service providers to store personal data. In some instances, these service providers may be located in countries with different data protection laws, which may make it difficult for organizations to guarantee the security of their consumer's data across different jurisdictions.

7. SOLUTION TO ADDRESS CHALLENGES ASSOCIATED WITH PROTECTING PRIVACY

To address these challenges, various potential solutions that can be explored include regular updates to measure security, effective data encryption, multi-factor authentication, and ultimately privacy by design. To address the challenge of cyber threats evolving constantly, organizations and companies need to constantly update their security measures to keep pace with the evolving cyber threats. Some of the ways this can be achieved are through implementing the latest security software and also regularly patching the existing vulnerabilities [12]. Another potential solution can be data encryption. This can be a crucial measure to protect personal data in digital spaces. And can be used by organizations with vast data storage to guarantee that their consumer's data is safe both during transit and rest [12]. Multi-factor authentication is also an essential feature that is very effective in protecting against unauthorized access to personal data. With extra layers of verification and identification, such as passwords, fingerprints, and scans, companies can guarantee the safety of their client's personal data [26].

Ultimately, Privacy by Design is a framework that seeks to integrate privacy and data security considerations into the design and development of digital systems and products. Privacy by Design emphasizes the need to prioritize data security and privacy from the outset of the design process rather than treating these issues as an afterthought [27]. Another example is the concept of "Privacy Engineering." Privacy Engineering is a framework that seeks to apply engineering principles and methodologies to the designs and development of privacy enhancements technologies and systems [28]. Privacy engineering emphasizes the need for rigorous testing and evaluation of data security measures, as well as the need for ongoing monitoring and updates to ensure that these measures remain effective over time.

8. CONCLUSION

In conclusion, the concept of privacy in computer ethics has become increasingly important as our lives become more interconnected with digital spaces. The five ethical considerations discussed in this essay provide a framework for ensuring that personal information is handled in a way that is ethical, responsible, and respectful of individuals' rights and privacy. The first ethical consideration is the concept of privacy itself. Privacy is essential for individuals to maintain control over their personal information and to protect their privacy rights. Without privacy, individuals may be at risk of identity theft, harassment, or other forms of harm. The second ethical consideration is consent. Individuals must be fully informed about how their personal information is being used and be able to give or refuse consent to use it. Consent must be freely given and informed without coercion or manipulation. The third ethical consideration is transparency. Organizations must be transparent about how they collect, use, and disclose personal information. Transparency helps to build trust between organizations and individuals and ensures that individuals have the information they need to make informed decisions about their personal information. The fourth ethical consideration is data protection. Organizations must take steps to protect personal information from unauthorized access, use, or disclosure. Data protection measures may include encryption, access controls, and secure storage and disposal of personal information. The fifth and final ethical consideration is data security. Organizations must take steps to ensure the security of personal information, including protecting against cyber-attacks, data breaches, and other security threats. Data security measures may include network security, anti-malware software, and regular security audits. In summary, the five ethical considerations related to privacy in computer ethics provide a comprehensive framework for promoting the responsible and ethical use of personal information in the digital space. By prioritizing privacy, consent, transparency, data protection, and data security, organizations can help to ensure that personal information is treated in a way that is consistent with ethical principles and respect for individuals' rights and privacy. As our lives become increasingly digitized, it is essential that we continue to prioritize these ethical considerations to protect personal information and promote ethical behavior in digital spaces.

REFERENCES

[1] T. R. Coles, "Does the privacy act of 1974 protect your right to privacy--an examination of the routine use exemption," *American University Law Review*, vol. 40, p. 957, 1990, [Online]. Available: http://heinonline.org/HOL/Page?handle=hein.journals/aulr40&id=975&div=&collection=journals%5Cnhttp://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1848&context=aulr%5Cnhttp://ezproxy.library.nyu.edu:2202/HOL/Page?handle=hein.journals/aulr40&div=44.

[2] J. A. Rothchild, "Against notice and choice: The Manifest failure of the proceduralist paradigm to protect privacy online (or anywhere else)," *Cleveland State Law Review*, vol. 66, no. 3, pp. 559–648, 2018.

[3] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, "Circumvention by design - Dark patterns in cookie consent for online news outlets," Oct. 2020, doi: 10.1145/3419249.3420132.

[4] R. F. Jørgensen and T. Desai, "Right to privacy meets online platforms: Exploring privacy complaints against Facebook and Google," *Nordic Journal of Human Rights*, vol. 35, no. 2, pp. 106–126, Apr. 2017, doi: 10.1080/18918131.2017.1314110.

[5] U. of Pennsylvania, "Internet privacy census: A tale of two realities," [Online]. Available: https://blog.seas.upenn.edu/u-s-census-data-vulnerable-to-attack-without-enhanced-privacy-measures/.

[6] P. R. Center, "Americans and privacy concerned, confused and lacking of control over their personal information," *Pew Research Center*, 2019, [Online]. Available: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[7] L. Ponemon, "Cost of data breach," *Ponemon Institute*, no. May, pp. 1–30, 2015, [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/.

[8] E. Union, "General data protection regulation," pp. 1–6, 2021, doi: 10.1145/3492323.3495620.

[9] R. S. Deora and D. Chudasama, "Brief study of cybercrime on an internet," *Journal of Communication Engineering & Systems*, vol. 11, no. 1, pp. 1–6, 2021, doi: 10.37591/JoCES.

[10] Norton, "Norton LifeLock cyber safety insights reports: Special edition global insights on cybersecurity and remote work," 2021, [Online]. Available: https://now.symassets.com/content/dam/norton/campa.

[11] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed consent: Studying GDPR consent notices in the field," in *Proceedings of the ACM Conference on Computer and Communications Security*, Nov. 2019, pp. 973–990, doi: 10.1145/3319535.3354212.

[12] S. Iovan and A.-A. Iovan, "From cyber threats to cyber risks," *Conflict in Cyber Space*, vol. 10, no. 2, pp. 43–60, 2021, doi: 10.4324/9781315669878-9.

[13] L. Taylor, "What is data justice? The case for connecting digital rights and freedoms globally," *Big Data and Society*, vol. 4, no. 2, p. 205395171773633, Nov. 2017, doi: 10.1177/2053951717736335.

[14] A. Vaccaro and P. Madsen, "Firm information transparency: Ethical questions in the information age," in *IFIP International Federation for Information Processing*, vol. 223, Springer {US}, 2006, pp. 145–156.

[15] I. Calzada, "Data spaces and democracy," *RSA Journal*, vol. 165, no. 2, pp. 40–43, 2019.

[16] Z. Tan *et al.*, "Enhancing big data security with collaborative intrusion detection," *IEEE Cloud Computing*, vol. 1, no. 3, pp. 27–33, Sep. 2014, doi: 10.1109/MCC.2014.53.

[17] A. Mantelero, "Competitive value of data protection: The impact of data protection regulation on online behaviour," *International Data Privacy Law*, vol. 3, no. 4, pp. 229–238, Jul. 2013, doi: 10.1093/idpl/ipt016.

[18] J. Herrle and J. Hirsh, "The Peril and Potential of the GDPR," *Arnoldia*, vol. 66, no. 4, pp. 2–12, 2009.

[19] J. Klemovitch, L. Sciabbarrasi, and A. Peslak, "Current privacy policy attitudes and fair information practice principles: A macro and micro analysis," *Issues In Information Systems*, vol. 22, no. 3, pp. 145–159, 2021, doi: 10.48009/3_iis_2021_159-174.

[20] A. Kashid, V. Kulkarni, and R. Patankar, "Discrimination prevention using privacy preserving techniques," *International Journal of Computer Applications*, vol. 120, no. 1, pp. 45–49, Jun. 2015, doi: 10.5120/21195-3860.

[21] N. T. Lee, "Detecting racial bias in algorithms and machine learning," *Journal of Information, Communication and Ethics in Society*, vol. 16, no. 3, pp. 252–260, Aug. 2018, doi: 10.1108/JICES-06-2018-0056.

[22] L. Taylor and L. Floridi, "Data ethics: The new frontier of applied ethics," *Philosophy & Technology*, vol. 29, no. 1, pp. 1–8, 2016, doi: 10.1098/rsta.2016.0360.

[23] M. Fadda *et al.*, "Ethical issues of collecting, storing, and analyzing geo-referenced tweets for mental health research," *Digital Health*, vol. 8, p. 205520762210925, Jan. 2022, doi: 10.1177/20552076221092539.

[24] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the top five evolving threats in cybersecurity: An in-depth overview," *Mesopotamian Journal of Cyber Security*, pp. 57–63, Mar. 2023, doi: 10.58496/mjcs/2023/010.

[25] N. Ž. Joksimović and S. Marinković, "SYMORG 2018 'Doing business in the digital age: challenges, approaches and solutions'-

Conference review," *Management: Journal of Sustainable Business & Management Solutions in Emerging Economies*, vol. 23, no. 2, pp. 1–3, 2018, [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=131674720&site=ehost-live&scope=site.

[26] D. Dasgupta, A. Roy, and A. Nag, "Multi-factor authentication," in *Infosys Science Foundation Series*, Springer International Publishing, 2017, pp. 185–233.

[27] I. S. Rubinstein, "Regulating privacy by design," *Berkeley Technology Law Journal*, vol. 26, no. 3, pp. 1409–1456, 2011, [Online]. Available: http://ra.ocls.ca/ra/login.aspx?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=74237061&site=eds-live.

[28] G. Danezis *et al.*, "Privacy and data protection by design - from policy to engineering," 2015, doi: 10.2824/38623.

BIOGRAPHIES OF AUTHORS

Robin Chataut is an assistant professor in the Department of Computer Science at Fitchburg State University, Massachusetts, USA. He obtained his undergraduate degree in Electronics and Communication Engineering from Pulchowk Campus, Tribhuvan University, Nepal in 2014, and his Ph.D. in Computer Science and Engineering from the University of North Texas, Texas, USA, in 2020. Prior to completing his Ph.D., he was a senior software developer for Jhilko Innovations, designing android apps for autistic children. His research interests are in the areas of wireless communication and networks, 5G, 6G, and beyond networks, vehicular communication, smart cities, Internet of Things, wireless sensor networks, and network security. He has designed, implemented, and optimized several algorithms and hardware architectures for precoding, detection, user scheduling, channel estimation, and pilot contamination mitigation for massive MIMO systems for 5G and beyond networks. He has authored and co-authored several research articles. He is an active reviewer in several international scientific journals and conferences. He can be contacted at email: rchataut@fitchburgstate.edu.

Maxwell Zostant holds an undergraduate degree in Computer Science with a concentration in Cyber Security from Fitchburg State University. Currently, Maxwell is gaining practical experience as an Information Technology Technian at Woodmeister Master Builders, where he is actively applying his knowledge and skills in a professional setting. With a keen interest in the fields of cybersecurity and computer networks, Maxwell has engaged in research to deepen his understanding of these crucial areas. His research endeavors have allowed him to explore the intricacies of securing computer systems and networks, ensuring the confidentiality, integrity, and availability of sensitive information. He can be contacted at email: maxzostant2298@gmail.com.