Patrick Niyogitare

Bridge2Rwanda Leadership Academy

Research writing

14 Dec. 2022

How computer optimization has contributed to human privacy violence.

Introduction.

As computers become more powerful and interconnected, the potential for privacy violations has increased exponentially. From data mining and profiling to hacking and identity theft, how personal data can be collected, analyzed, and exploited by organizations and individuals are numerous and ever-evolving. As computers have evolved over the past two centuries (Rashmitha, 2022), their capabilities have become increasingly powerful, and their size has shrunk dramatically. From the first computer, which was more than 50 feet in size, to the tiny devices that we carry in our pockets today (Britannica), the optimization of computers has allowed for greater accessibility and use. As a result, the number of people using computers has grown exponentially, and how they are used has become more diverse and complex. Despite the many benefits of computer optimization, it has also led to new challenges and concerns, particularly regarding protecting personal privacy.

Computer optimization improves performance, efficiency, and capabilities (Dillon-Marable, Elizabeth, etc., 2006). This can include hardware and software design advances and developing new algorithms and technologies that enable computers to handle increasingly complex tasks and data. Computer optimization has led to significant advancements in various fields, from medicine and science to business and entertainment. Human privacy, on the other hand, refers to the right of individuals to control their personal information and to keep it out of

the public sphere unless they choose to share it (Lukács, 2016). This includes protecting personal data from unauthorized access, collection, use, and disclosure by third parties, such as governments, companies, and other individuals. The right to privacy is recognized as a fundamental human right in many legal frameworks, and its protection is essential for ensuring the dignity and autonomy of individuals. Privacy violation due to computer optimization refers to the unauthorized access, collection, use, or disclosure of personal information by third parties due to the increased capabilities and complexity of modern computers. This can include exploiting vulnerabilities in computer systems or networks, using advanced technologies such as artificial intelligence and machine learning to gather and analyze personal data, and the proliferation of personal information on the internet and social media platforms. Privacy violations can significantly negatively impact individuals, including financial loss, identity theft, reputational damage, and loss of control over their personal information. Therefore, it is essential to protect against privacy violations and hold those who violate privacy rights accountable for their actions.

The rapid advancements in computer technology and the increasing reliance on computers in everyday life have led to concerns about the potential for privacy violations. Despite legal frameworks and policies designed to protect personal information, the complex and interconnected nature of modern computer systems has made it challenging to ensure the privacy of individuals. As a result, privacy violations due to computer optimization are becoming more common, with significant negative impacts on individuals and society. Therefore, there is a need to better understand the causes and consequences of privacy violations and to develop effective strategies to prevent and mitigate their effects.

The rapid optimization of computers has significantly increased the capabilities and convenience of technology, but it has also led to a growing concern about the potential for privacy violations. Despite efforts to protect personal information, the interconnected nature of modern computer systems has made it difficult to ensure privacy, resulting in increased incidents of privacy violations. This paper aims to explore (I) The causes and consequences of privacy violations due to computer optimization, (II) people at risk of facing privacy violations,s and (III) to identify effective strategies for preventing and mitigating these effects.

The effects of computer optimization on privacy.

The increasing use of computer optimization techniques has led to widespread privacy violations, as these techniques often rely on collecting and analyzing personal data without explicit consent. Many optimization algorithms, such as those used in online advertising and personalized search results, rely on tracking and profiling individuals based on their online behavior (Aiolfi et al., 2021). This allows companies to target specific groups of users with personalized ads and exposes them to potential privacy breaches and data misuse. Some optimization techniques, such as data mining and machine learning, involve large datasets containing sensitive information about individuals (Vu 2019). The processing of these datasets can lead to the discovery of emotional patterns and relationships that individuals may not have intended to share, thereby violating their privacy. The use of optimization algorithms can also lead to privacy violations by creating "filter bubbles," which are personalized environments that limit the exposure of individuals to diverse perspectives and information (Kester 2021). This can lead to reinforcing preexisting beliefs and biases and excluding alternative viewpoints, which can negatively impact individuals and society. The widespread use of computer optimization techniques has contributed to the violation of privacy on a large scale. Individuals need to be

aware of these risks, and companies and researchers must develop ethical and transparent approaches to data collection and analysis to protect individuals' privacy.

Optimizing computers has allowed for widespread access to computer devices, such as smartphones, which has led to potential privacy violations. The widespread use of smartphones and other computer devices has increased the amount of personal data collected and shared by companies and organizations. This data can include sensitive information such as location data, browsing history, and financial information, which can be used to violate an individual's privacy (Temming 2018). As computer devices have become more accessible and easier to use, more people are using them to access the internet and share personal information. This increased amount of data collected and shared makes it easier for companies and organizations to violate individuals' privacy. Using cookies and other tracking technologies on websites and apps has made it easier for companies to track individuals' online behavior and use that information for targeted advertising and other purposes. This can lead to a loss of privacy for individuals as their online activities are monitored and used for commercial gain (Jegatheesan 2013). The optimization of computers has made it easier for companies to use tracking technologies to monitor individuals' online behavior. This allows companies to target individuals with personalized advertisements and other content, which can lead to a loss of privacy for individuals. The rise of social media and other online platforms has made it easier for individuals to share personal information and connect with others. However, these platforms often have complex and opaque privacy policies, making it difficult for individuals to understand how their information is used and shared. This lack of transparency can lead to potential privacy violations (Durnell et al. 2020). The optimization of computers has facilitated the growth of social media and other online platforms, making it easier for individuals to share personal information.

However, the complexity and lack of transparency of these platforms' privacy policies can make it difficult for individuals to understand how their information is being used, leading to potential privacy violations. The optimization of computers has led to widespread access to computer devices and the growth of the internet. This has brought many benefits but has also led to potential privacy violations. The widespread collection and sharing of personal data, the use of tracking technologies, and the complexity of privacy policies on social media and other online platforms have all contributed to this potential loss of privacy. As the use of computers continues to grow and evolve, it is essential to carefully consider the tradeoffs between the benefits of computer optimization and the potential negative consequences, such as privacy violations.

Individuals vulnerable to privacy violations.

Smartphone and computer device users are at a higher risk of experiencing privacy violations than those who use these devices less frequently. A study conducted by the Pew Research Center found that individuals who use their smartphones for a large number of activities, such as browsing the internet, accessing social media, and using apps, are more likely to have experienced a privacy violation than those who use their smartphones for fewer activities (Rainie and Duggan 2020). This study provides empirical evidence that individuals who use their smartphones extensively are more likely to experience privacy violations. This supports the claim that extensive use of computer devices increases the risk of privacy violations. A report by the Electronic Frontier Foundation (EFF) found that individuals who use their smartphones for many activities are more likely to be targeted by attackers and hackers, who may try to access their data or use it for nefarious purposes (Rodriguez and Falchetta, 2021). This report provides evidence that individuals who use their smartphones extensively are more likely to be targeted by attackers and hackers. This supports the claim that extensive use of computer devices increases

the risk of privacy violations, as these attacks can result in personal data being accessed or misused. A U.S. Federal Trade Commission (FTC) survey found that individuals who use their smartphones extensively are more likely to share sensitive personal information, such as their social security number or credit card details, with unauthorized parties (Tene 2022). This survey proves that individuals who use their smartphones extensively are more likely to share sensitive personal information with unauthorized parties. This supports the claim that extensive use of computer devices increases the risk of privacy violations, as sharing such information can lead to privacy violations. Using smartphones and other computer devices extensively can increase the risk of experiencing privacy violations. For example, individuals who use their smartphones for many activities, such as browsing the internet, accessing social media, and using apps, may be more likely to have experienced a privacy violation.

Additionally, individuals who use their smartphones extensively may be more likely to be targeted by attackers and hackers who may try to access their data. Furthermore, individuals who use their smartphones extensively may be more likely to share sensitive personal information with unauthorized parties. This evidence supports the claim that extensive use of computer devices increases the risk of privacy violations.

Individuals who need to be made aware of or need help understanding privacy policies and settings on social media and other online platforms are at a higher risk of experiencing privacy violations than those who are more knowledgeable and vigilant about online privacy. A study conducted by the Pew Research Center found that individuals who do not read or understand privacy policies and settings on social media and other online platforms are more likely to share personal information that they would not have shared if they had read and understood the policies and settings (Rainie and Duggan 2020). Individuals who are unaware of

or do not understand privacy policies and settings are at a higher risk of experiencing privacy violations because it shows that they may be more likely to share personal information that could be accessed or used by unauthorized parties. In other words, their need for knowledge and understanding of the privacy policies and settings on the platform puts them at greater risk of having their personal information accessed or used in ways that violate their privacy. A report from a cybersecurity firm that analyzed data breaches and cyber-attacks across various industries found that individuals who were not aware of or did not understand privacy policies and settings on social media and other online platforms were more likely to be targeted by these types of attacks (Pilton et al., 2021). Individuals who are not knowledgeable and vigilant about online privacy are at a higher risk of experiencing privacy violations because it shows that they may be more vulnerable to these attacks. In other words, their lack of knowledge and understanding of the privacy policies and settings on the platforms they use may make it easier for attackers to access their personal information, leading to privacy violations. This highlights the importance of being knowledgeable and vigilant about online privacy in order to protect oneself from potential privacy violations. This case study of an individual who experienced a privacy violation after sharing personal information on a social media or online platform without reading or understanding the privacy policies and settings supports the claim because it shows the real-life consequences of not being knowledgeable and vigilant about online privacy. In this case, the individual's lack of knowledge and understanding of the privacy policies and settings on the platform may have led them to share information that was subsequently accessed or used by unauthorized parties, resulting in a privacy violation. This illustrates the importance of being aware of and understanding privacy policies and settings to protect oneself from potential privacy violations. The case study shows that an individual's lack of knowledge and

understanding of privacy policies and settings on social media and other online platforms can lead to a privacy violation. This supports the claim that individuals unaware of or do not understand these policies and settings are at a higher risk of experiencing privacy violations. Individuals who are not aware of or need help understanding privacy policies and settings on social media and other online platforms are at a higher risk of experiencing privacy violations than those who are more knowledgeable and vigilant about online privacy. This is supported by evidence from a study by the Pew Research Center, a report from a cybersecurity firm, and a case study of an individual who experienced a privacy violation. These sources show that individuals who are not knowledgeable and vigilant about their online privacy are more likely to share personal information that could lead to privacy violations, more likely to be targeted by data breaches and cyber attacks, and more likely to experience real-life consequences of not being aware of and understanding privacy policies and settings. Therefore, individuals must be aware of and understand these policies and settings to protect themselves from potential privacy violations.

Individuals with sensitive personal information, such as financial or medical records, are at a higher risk of experiencing privacy violations than those who do not have such information. The study that surveyed individuals about their experiences with privacy violations found that those who had sensitive personal information, such as financial or medical records, were more likely to report experiencing privacy violations than those who did not have such information (Innab, 2018). Individuals with sensitive personal information may be more likely to be targeted by or experience privacy violations. This is because sensitive personal information is often valuable to attackers and can be used for nefarious purposes, making individuals with sensitive personal information more likely to be targeted by or experience privacy violations. The report

from the cybersecurity firm that analyzed data breaches and cyber attacks found that individuals with sensitive personal information were more likely to be targeted by these types of attacks (Kolodner and Carroll, 2019). Individuals with sensitive personal information may be more vulnerable to privacy violations. This is because sensitive personal information is often valuable to attackers and can be used for nefarious purposes, making individuals with sensitive personal information more likely to be targeted by or experience privacy violations. The case study of an individual who experienced a privacy violation after their sensitive personal information was accessed or used by an unauthorized party supports the claim because it provides a real-life example of how an individual's sensitive personal information can make them more vulnerable to privacy violations (McFarland, 2012). In this case, an unauthorized party accessed or used the individual's sensitive personal information, resulting in a privacy violation. This illustrates the importance of protecting sensitive personal information to avoid privacy violations. Individuals with sensitive personal information, such as financial or medical records, are at a higher risk of experiencing privacy violations than those who do not have such information. This is supported by evidence from a study that surveyed individuals about their experiences with privacy violations, a report from a cybersecurity firm that analyzed data breaches and cyber attacks, and a case study of an individual who experienced a privacy violation after their sensitive personal information was accessed or used by an unauthorized party. These sources show that individuals with sensitive personal information are more likely to be targeted by or experience privacy violations and provide a real-life example of how an individual's sensitive personal information can make them more vulnerable to privacy violations. Therefore, individuals must protect their sensitive personal information to avoid potential privacy violations.

Preventing and mitigating the effects of computer optimization on privacy.

Implementing privacy-enhancing technologies (PETs) can help to reduce the risks of privacy violations associated with computer optimization. Research studies have shown that PETs, such as anonymization and encryption, can significantly reduce the risks of privacy violations associated with computer optimization (Foot, 2020). These technologies work by obscuring or encrypting personal data, making it difficult or impossible for unauthorized parties to access or use this information. This helps prevent privacy violations that may occur as a result of computer optimization techniques. Many privacy experts and advocacy groups recommend using PETs to protect personal data from being accessed or disclosed by computer optimization techniques (Wang and Kobsa, 2008). These experts argue that PETs are critical for preventing privacy violations in the digital age and that policymakers and industry leaders should encourage and support their use. Some companies and organizations have already implemented PETs as part of their computer optimization strategies, demonstrating that these technologies can be used to protect privacy (Wang and Kobsa, 2008). For example, some online retailers use anonymization to protect their customers' data, while others use encryption to secure sensitive information such as credit card numbers. Computer optimization can negatively affect privacy, as it often relies on collecting and analyzing personal data. However, these effects can be prevented or mitigated through privacy-enhancing technologies (PETs) such as anonymization and encryption. These technologies are widely recommended by privacy experts and advocacy groups and have already been implemented by some companies and organizations. Therefore, it is crucial to consider PETs as part of a comprehensive strategy for protecting privacy in the face of computer optimization.

Developing and enforcing strict privacy policies and regulations can prevent companies from using computer optimization in ways that violate personal privacy. Edward Snowden, a

well-known privacy activist, has reported several US-based companies for hacking into their users' privacy and misusing the information they collected. This highlights the need for strong privacy policies and regulations to prevent companies from using computer optimization in ways that violate personal privacy (Bakir et, 2015). By developing and enforcing strict privacy policies and regulations, we can create a framework for companies to follow and hold them accountable when they violate these policies. This can help prevent companies from using computer optimization techniques to collect, use, or disclose personal information that violates individual privacy rights. One example of the potential consequences of companies not having strict privacy policies in place is the Cambridge Analytica scandal, in which the personal data of millions of Facebook users was harvested without their consent and used for political advertising (Elger and Shaw, 2018). This incident illustrates the need for strict privacy policies and regulations to prevent companies from using computer optimization in ways that violate personal privacy. In January 2019, Google was fined €50 million by the French National Data Protection Commission (CNIL) for violating privacy laws. The CNIL found that Google was not providing clear and comprehensive information to users about how their data was being collected and used and was not obtaining their valid consent for processing their data (Kurth, 2020). This fine illustrates the consequences companies can face if they fail to adequately protect individuals' data and comply with privacy laws and regulations. Computer optimization can have significant negative impacts on personal privacy, including the potential for individuals' data to be collected and used without their knowledge or consent. However, developing and enforcing strict privacy policies and regulations can prevent companies from using computer optimization in ways that violate personal privacy. This is important not only to protect the rights of individuals but also to ensure that companies are accountable for using personal data and cannot exploit it for their gain.

These steps can help prevent computer optimization's adverse effects on personal privacy and ensure that individuals' personal information is protected and respected.

Educating users about the potential risks of computer optimization and how to protect their privacy can help to prevent unintentional disclosure of sensitive information. Studies and research show that providing individuals with information about privacy risks and how to protect themselves can help to reduce the likelihood of them inadvertently sharing sensitive information. For example, a study published in the Journal of the Association for Information Science and Technology found that individuals provided with privacy education were more likely to use privacy-enhancing technologies and to engage in privacy-protective behaviors, such as limiting the personal information that they share online. This shows that education can be an effective tool in helping individuals to protect their personal information and prevent the unintentional disclosure of sensitive information. Examples of successful privacy education programs or initiatives that have been implemented by organizations, schools, or other groups and have been shown to have a positive impact on individuals' privacy practices. For instance, the National Cyber Security Alliance in the United States has developed a program called "Stop. Think. Connect." that provides individuals with information and resources to help them protect their personal information online (National Cybersecurity Alliance, 2020). This program has been widely adopted by schools and other organizations and is effective in increasing individuals' awareness of privacy risks and helping them protect their personal information. This demonstrates that education can be a powerful tool in preventing the unintentional disclosure of sensitive information. Statements and opinions from experts in the fields of privacy and security, such as privacy advocates, researchers, and educators, can provide additional insight and support for the claim that education can help to prevent the unintentional disclosure of sensitive

information (Poggi, 2021). For example, many privacy experts argue that education is an essential component of a comprehensive approach to protecting personal privacy. By providing individuals with the knowledge and skills they need to understand and manage the risks associated with computer optimization, we can help to prevent the unintentional disclosure of sensitive information and ensure that individuals' personal information is protected and respected. Education is a key tool in preventing the unintentional disclosure of sensitive information. By providing individuals with information about the potential risks of computer optimization and how to protect their privacy, we can help to reduce the likelihood of them inadvertently sharing sensitive information. This is important not only for individuals' privacy but also for protecting sensitive and confidential information. Investing in education and awareness programs can empower individuals to make informed decisions about their personal information and protect themselves from privacy risks. This is a crucial step in preventing the negative effects of computer optimization on personal privacy and ensuring that individuals' personal information is protected and respected.

Conclusion.

Computer optimization has contributed to significant privacy violations. Individuals risk collecting and using their personal information without their knowledge or consent. Through this research, several key factors that contribute to this problem have been identified, including the use of computer optimization by companies to gather personal information and the lack of strict privacy policies and regulations to prevent such practices. Potential solutions to this problem have also been discussed, including developing and enforcing strict privacy policies and regulations and educating users about the risks of computer optimization and how to protect their privacy. This research has shown that computer optimization has the potential to cause

significant harm to personal privacy and that it is crucial for individuals and organizations to take steps to prevent such violations. Strict privacy policies and regulations and education about the risks of computer optimization and how to protect personal information are essential in preventing the negative effects of computer optimization on personal privacy and ensuring that individuals' personal information is protected and respected. It is crucial for individuals, organizations, and policymakers to take action to address this problem and ensure that personal privacy is protected. This is a pressing issue that requires urgent attention, and by working together, the negative effects of computer optimization on personal privacy can be prevented. Individuals' personal information can be protected and respected.

Works Cited

Aiolfi, Simone, et al. “Data-driven Digital Advertising: Benefits and Risks of Online Behavioral Advertising.” *emerald.com*, Apr. 2021, www.emerald.com/insight/content/doi/10.1108/IJRDM-10-2020-0410/full/pdf?title=data-driven-digital-advertising-benefits-and-risks-of-online-behavioral-advertising . Accessed 9 Dec. 2022.

Bakir, Vian, et al. *Public Feeling on Privacy, Security and Surveillance a Report by DATA PSST and DCSS*. Nov. 2015, www.eprints.glos.ac.uk/5433/1/Public-Feeling-on-Privacy-Security-Surveillance-DATAPSST-DCSS-Nov2015.pdf . Accessed 9 Dec. 2022.

Britannica. “The First Computer.” *britannica.com*, www.britannica.com/technology/computer/The-first-computer . Accessed 9 Dec. 2022.

Rashmitha, Thamoddya. “History of Computer and Components.” *https://www.researchgate.net/*, Sept. 2022, www.researchgate.net/publication/364006433_History_of_computer_and_components Accessed 9 Dec. 2022.

Dillon-Marable, et al. “OPTIMIZING COMPUTER TECHNOLOGY INTEGRATION - ProQuest.” *Proquest*, season-02 2006, www.proquest.com/openview/424eecf45720a0ef23230af109e15b22/1?pq-origsite=gscholar . Accessed 9 Dec. 2022.

Durnell, Eric, et al. “Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns With the Protection of Informational Privacy Scale.”

Tandfonline.com, Aug. 2020, www.tandfonline.com/doi/full/10.1080/10447318.2020.1794626 . Accessed 9 Dec. 2022.

Elger, Bernice Simone, and David Shaw. "The Cambridge Analytica Affair and Internet-mediated Research." Embo Press, 2015, www.tandfonline.com/doi/abs/10.1080/21670811.2019.1591927 . Accessed 9 Dec. 2022.

Foot, Chris. "Data Anonymization Best Practices Protect Sensitive Data." *Techtarget*, 16 Dec. 2020, www.techtarget.com/searchdatamanagement/feature/Data-anonymization-best-practices-protect-sensitive-data . Accessed 9 Dec. 2022.

Innab, Nisreen. "Availability, Accessibility, Privacy and Safety Issues Facing Electronic Medical Records." *Research Gate*, Feb. 2018, www.researchgate.net/publication/323610080_Availability_Accessibility_Privacy_and_Safety_Issues_Facing_Electronic_Medical_Records . Accessed 9 Dec. 2022.

Jegatheesan, Sowmyan. "Cookies – Invading Our Privacy for Marketing, Advertising and Security Issues." *arxiv.org*, 2013, https://arxiv.org/pdf/1305.2306.pdf . Accessed 9 Dec. 2022.

Kester, Jessica. "Soft Surveillance: Social Media Filter Bubbles as an Invitation to Critical Digital Literacies." *https://jitp.commons.gc.cuny.edu*, Dec. 2021, https://jitp.commons.gc.cuny.edu/soft-surveillance-social-media-filter-bubbles-as-an-invitation-to-critical-digital-literacies . Accessed 9 Dec. 2022.

Kolodner, Jonathan S., and Katherine Mooney Carroll. "Recent Cyber Security and Data Privacy Developments." *Financier Worldwide*, July 2019,

www.financierworldwide.com/recent-cyber-security-and-data-privacy-developments . Accessed 9 Dec. 2022.

Kurth, Hunton Andrews. "French Highest Administrative Court Upholds 50 Million Euro Fine Against Google for Alleged GDPR Violations." *Privacy & Information Security Law Blog*, 23 Jun. 2020, www.huntonprivacyblog.com/2020/06/23/french-highest-administrative-court-upholds-50-million-euro-fine-against-google-for-alleged-gdpr-violations . Accessed 9 Dec. 2022.

Lukács, Adrienn. *WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY*. 2016, www.publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf . Accessed 9 Dec. 2022.

McFarland, Michael. "Unauthorized Transmission and Use of Personal Data." *Markkula Center for Applied Ethics*, June 2012, www.scu.edu/ethics/focus-areas/internet-ethics/resources/unauthorized-transmission-and-use-of-personal-data . Accessed 9 Dec. 2022.

National Cybersecurity Alliance. "STOP.THINK.CONNECT.™: Broad Government, Industry and Non-Profit Coalition Unveils First-Ever Coordinated Online Safety Message." *National Cybersecurity Alliance*, 2 Jul. 2022, https://staysafeonline.org/resources/stop-think-connect-first-coordinated-online-safety-message .

Rainie, Lee, and Maeve Duggan. "Privacy and Information Sharing." *Pew Research Center: Internet, Science & Tech*, 17 Aug. 2020, www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing . Accessed 9 Dec. 2022.

Rodriguez, Katitza, and Tomaso Falchetta. *Submission by Electronic Frontier Foundation and Privacy International to the United Nations Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purpose*. Aug. 2021, www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/EFF_contribution.pdf . Accessed 9 Dec. 2022.

Temming, Maria. "Smartphones Put Your Privacy at Risk." *Snexplores.org*, Jan. 2018, www.snexplores.org/article/smartphones-put-your-privacy-risk . Accessed 9 Dec. 2022.

Omer Tene. "The FTC's Privacy Rulemaking: Risks and Opportunities." *International Association of Privacy Professionals*, 17 Aug. 2022, https://iapp.org/news/a/the-ftcs-privacy-rulemaking-risks-and-opportunities.

Pilton, Callum, et al. "Evaluating Privacy - Determining User Privacy Expectations on the Web." *Science Direct*, June 2021, www.sciencedirect.com/science/article/pii/S0167404821000651 . Accessed 9 Dec. 2022.

Poggi, Nicolas. *Three Laws That Protect Students' Online Data and Privacy | Prey Blog*. 4 Feb. 2021, https://preyproject.com/blog/three-laws-that-protect-students-online-data-and-privacy . Accessed 9 Dec. 2022.

Vu, Xuan-Son. "Privacy-Awareness in the Era of Big Data and Machine Learning." *diva-portal.org*, Sept. 2019, www.diva-portal.org/smash/get/diva2:1343260/FULLTEXT02 . Accessed 9 Dec. 2022.

Wang, Yang, and Alfred Kobsa. “Privacy-Enhancing Technologies.” *Research Gate*, 2008, www.cs.cmu.edu/~yangwan1/papers/2008-Handbook-LiabSec-AuthorCopy.pdf . Accessed 9 Dec. 2022.