Navigating the Digital Privacy Paradox: Balancing Security, Surveillance, and User Control in the Modern Era

Daniel Thomas
daniel.cromwel@gmail.com

***Abstract*—As technological advancements continue to permeate daily life, the concept of privacy has become increasingly complex and contentious. This paper explores the evolving dynamics between privacy, security, and surveillance in the digital age. By examining both protective measures, such as data anonymization and encryption, and the increasing capabilities of surveillance technologies, it delves into the conflict between safeguarding personal information and maintaining public security. The study analyzes key privacy-enhancing technologies (PETs) such as k-anonymity, encryption methodologies, and collaborative machine learning, emphasizing their role in fortifying user data against breaches. Simultaneously, the paper critiques the intrusiveness of governmental surveillance and the ethical implications of its widespread use. Ultimately, it reflects on the trade-offs individuals must navigate between retaining control over personal data and enjoying the conveniences of modern technology. Despite advancements in privacy protection techniques, the paper concludes that while complete privacy may be an unattainable ideal, users can still mitigate risks through proactive data management and strategic engagement with privacy-enhancing tools.**

I. Introduction

In today's world, where technology plays a dominant role in daily life, the risk of a complete loss of privacy is greater than ever before. The definition of privacy has evolved throughout human history, and its meaning depends on the context. In the realm of technology and cyberspace, privacy often includes managing and controlling how one's personal data is shared and handled. However, complete privacy goes beyond these measures, as other factors—such as surveillance, data breaches, and third-party access—also contribute to the overall challenge of safeguarding privacy. While users may exercise control over their data, full absolute privacy remains elusive due to these additional complexities. Achieving privacy in the digital age is getting more and more challenging, as users' data is continuously collected, personal information is tracked, and actions are monitored ([1]).

It is often argued that tracking personal information by governmental institutions is reasonable and necessary. The widespread use of personal data, video surveillance, communication interception, and biometric devices is viewed as essential for maintaining public safety. Data protection laws provide exceptions to certain rules when crime prevention, detection, and national security are at stake ([1]). However, there is an ongoing debate about finding the right balance between users' privacy rights and the societal benefits of crime prevention and increased efficiency in official procedures.

As the threat of personal data breaches becomes more severe, effective solutions to address these concerns must also be implemented ([2]). This paper will examine whether current privacy protection efforts are truly effective and whether it is reasonable to expect privacy in today's world, where total privacy may no longer be achievable.

II. Privacy-Enhancing Technologies: Safeguarding Personal Data Against Privacy Leaks

In this digital age, there are lots of PETs that include both technical and organizational approaches designed to protect personal identity. From an organizational perspective, PETs provide industry guidelines that outline strategies for privacy protection. On the technical side, as the name suggests, PETs comprise a collection of technologies that safeguard individual privacy and minimize the collection of personal data by organizations. ([3]) Several PET methods are widely employed in privacy protection:

A. Data Anonymization

Data anonymization is an effective technique for preserving privacy. This method protects Personally Identifiable Information (PII) by concealing individuals' identities and personal details. Depending on the implementation, it can provide users with either complete anonymity or reversible pseudonymity. ([4]) Within user data, certain combinations of features, known as quasi-identifiers, can potentially be used to uniquely identify individuals. To reduce this risk, k-anonymity has become a widely adopted data anonymization method. This technique focuses on anonymizing quasi-identifiers by ensuring that each record is identical to at least k-1 other records in the dataset. Consequently, even if a data match occurs, it becomes difficult to identify a specific individual, as the information could relate to any one of at least k individuals ([5]).

Five core technologies are employed in this approach to data anonymization:

1) Generalization: This technique involves replacing or removing sensitive information with less specific data to ensure an individual's identity is no longer unique. Some original values are retained, which adds an element of confusion to the data.

2) Suppression: This method is applied to columns or tuples, replacing data with meaningless values to hide or remove certain parts of the information.
3) Swapping: This process involves randomly rearranging variables within each column to disrupt the original data structure.
4) Masking: This technique alters specific characters by replacing them with different characters, preserving the data format while obscuring the actual values.
5) Distortion: This method involves altering data in a way that is reversible using the original data, allowing for data protection during storage or transmission while maintaining the ability to recover the original information when necessary.

The fundamental principle of these technologies is to reduce the correlation between input and output data, thereby safeguarding user privacy while maintaining data utility. This approach effectively balances the need for data protection with the requirement for meaningful information retention.

B. Encryption

Unlike traditional privacy protection methods that depend on privacy policies and system administrators, encryption enhances data security and reduces the need to trust individuals. This is achieved by employing encryption algorithms to replace the need for third-party oversight. ([6]) Encryption can be broadly categorized into two main types: symmetric and asymmetric. Symmetric encryption employs a single secret key shared between two parties to ensure communication security. As long as the secret key remains undisclosed, only authorized parties can access the information, thus preventing data leaks. In contrast, asymmetric encryption utilizes a pair of keys: a private key and a public key. Users can receive encrypted messages from the public using the public key, but only the private key can decrypt these messages, ensuring data confidentiality. Additionally, asymmetric encryption provides digital signatures to verify the identities of communicating parties, thereby preventing message tampering. The fundamental difference lies in their accessibility; the private key is exclusively owned by an individual, while the public key is openly available to everyone ([7]). A comparison of these two encryption types reveals distinct characteristics. Symmetric encryption generally employs smaller key sizes, potentially making it less secure for highly sensitive information. On the other hand, asymmetric encryption requires more computational resources when handling large volumes of data, leading to increased complexity. The selection of an appropriate encryption method is primarily determined by the specific attributes and security requirements of the data in question. Furthermore, a combination of symmetric and asymmetric encryption, known as hybrid encryption, utilizes the strengths of both methods to enhance both speed and security. One widely adopted application of this approach is end-to-end encryption (E2EE), which is commonly used in messaging applications. For instance, WhatsApp implements E2EE technology to ensure that only the sender and receiver can read or modify messages, thereby protecting user privacy even from service providers. In late 2021, WhatsApp expanded its E2EE security features, allowing users to restore their backup keys using a password, even if their device is lost. Millions of users have chosen to utilize this enhanced security measure ([8]). In summary, encryption protects privacy by converting data into a coded form, ensuring only authorized parties can access the information, thus safeguarding users' personal data from unauthorized access.

C. Collaborative ML approaches

The combination of PETs with Machine Learning (ML) aims to transform sensitive data into valuable information through ML techniques while either revealing only data permitted by concerned parties or without exposing any information to third parties. Federated Learning (FL) is one of the most widely adopted Collaborative Machine Learning approaches. This method enables users to train models locally on their own devices, with only model updates being transmitted to a central server rather than raw data. As the raw data remains stored exclusively on the user's device, even if the central server is compromised, attackers cannot access users' private information, thus significantly reducing the risk of privacy breaches. In contrast to centralized training methods, Collaborative Machine Learning approaches allow models to learn cooperatively without compromising data privacy ([9]). Overall, these collaborative approaches to machine learning represent a significant advancement in data privacy protection. By allowing valuable insights to be gained without compromising individual privacy, they address critical concerns in the evolving landscape of data security.

III. The Shatter of Privacy: Privacy-Invading and Technologies Crushing Through PETs

Although PETs seem able to protect most of the security, while valuable, they have limitations and cannot fully protect privacy in every context. According to the article from Frontiers in Public Health, PETs like differential privacy, federated learning, and homomorphic encryption face challenges such as balancing privacy with data utility and addressing re-identification risks. The wide array of definitions, terminology, and actors makes it difficult to identify sources for privacy engineering benchmarking and expertise, which complicates their consistent application and effectiveness across various data environments ([10]). This demonstrates the complexity and limitation of relying solely on PETs for comprehensive privacy protection.

A. Cracking your device and privacy: Hacking technology

One of the great threats to personal privacy is malicious hacking from others, causing the leak or even loss of sensitive data. Unfortunately, the current PETs are not perfect to prevent all the hacks. Here, I am going to introduce the hacking technologies that kill privacy. A popular way of hacking is Hacking Internet of Things (IoT) devices, such as printers,

which pose a significant cybersecurity threat due to the often-overlooked vulnerabilities in these connected devices. Printers are increasingly being targeted by cybercriminals who exploit their security weaknesses to gain unauthorized access to sensitive information or to use them as entry points into broader networks. Many printers are managed using web-based admin consoles that frequently have default usernames and passwords, making them easy targets for attackers. Poorly secured printers can serve as gateways for hackers to gain access to a network, steal sensitive data, or even launch a ransomware attack ([11]). Furthermore, modern printers store sensitive information, such as scanned documents and user credentials, which are the sensitive data of an enterprise or individuals.

In the broader context of IoT hacking, the challenges are even more significant. Not only the printer, IoT devices often have limited computational power and security features, making them attractive targets for hackers. Many IoT devices, including printers, lack robust encryption or secure authentication mechanisms, which allows attackers to exploit these vulnerabilities for malicious purposes. These vulnerabilities still exist in great numbers. According to a study on IoT security, the heterogeneous nature of IoT devices and the lack of a standardized security framework make them highly susceptible to a variety of attacks, including man-in-the-middle attacks, distributed denial-of-service, and unauthorized data access ([12]). Hackers can infiltrate IoT networks by using known exploits or vulnerabilities, enabling them to monitor communications, steal data, or even manipulate the functionality of the devices themselves.

B. Unwilled Data collection, leak, and surveillance Tech

Not only is privacy broken by invading technologies, but Wiretapping technology also damages personal privacy for the sake of surveillance, as it allows for the covert interception of private communications. Traditionally, wiretapping involved physically accessing telecommunication networks to listen in on phone calls or read text messages. "[W]iretap interfaces in telephone networks were compromised, leading to unauthorized interceptions" ([13]). These newer methods of wiretapping enable agencies to bypass traditional security and encryption measures, directly accessing data on individual devices. The installation of malware or spyware on targeted devices can covertly monitor all forms of digital communication, from emails to social media activities, while avoiding detection by conventional network security tools ([13]).

Also, the collection and use of user data by websites and organizations often result in significant privacy concerns, particularly when the data is collected without agreement or used for malicious purposes. While data collection is often justified to enhance user experience or personalize content, it frequently leads to privacy failures that can have far-reaching consequences for individuals. A direct example will be that after you fill in your phone on some website, you start to receive random fraud calls. Websites employ various methods to track and collect user data, including cookies and browser fingerprinting, to monitor online activities and gather detailed profiles of users. Web tracking techniques collect a variety of information, such as browsing behavior, personal preferences, or even age and income (Socket, n.d.). This data can be misused in several ways, from targeted advertising that manipulates user behavior to more illegal activities such as identity theft.

Privacy concerns are magnified when this data is shared or sold to third parties without users' knowledge. "[T]he commodification of personal data and its trade in largely unregulated markets can lead to significant privacy breaches, where user data is exposed to unauthorized entities, increasing the risk of exploitation" ([14]). The Optus data leak in 2022 is a typical example of how user data collection can lead to severe privacy breaches. In this accident, the personal information of around 10 million customers, including names, birthdates, addresses, and contact details, was exposed by a cyberattack due to poor security. "Optus' mishandling of customer information, such as storing data for longer than legally required, has raised significant questions about corporate responsibility and data governance" ([15]). The breach has demonstrated how inadequate security measures can lead to massive privacy violations and significant harm to individuals whose data is compromised. There are so many invading technologies and surveillance technologies stealing sensitive information from us and killing privacy.

IV. The Dual Edge of Privacy-Invading Technologies: Control, Security, and Public Trust

In the digital age, privacy-invading technologies have become indispensable tools for not only cybercrimes but also authorities, governments, and corporations alike. There are several key motivations behind their widespread use, each deeply rooted in maintaining control, ensuring security, and upholding societal order.

A. Power and Control

Governments, particularly authoritarian regimes, often use surveillance technologies to maintain control over their populations in a blatant and coercive manner. These regimes leverage advanced surveillance systems not just for the purpose of maintaining social order but also to strengthen their hold on power by systematically monitoring, censoring, and repressing any potential threats or opposition ([16]). By employing these tools, they create an environment where dissent becomes nearly impossible without significant risk.

China and Iran are often cited as the most sophisticated examples of state surveillance. The Chinese Communist Party uses a variety of privacy-invading technologies to monitor its citizens ([17]). The Great Firewall of China is a prime example, which functions as a nationwide censorship and surveillance system. This massive digital infrastructure blocks access to many foreign websites restricts the flow of information and monitors all internet activity within the country. Chinese authorities can track and censor social media

posts, email communications, and online searches, ensuring that dissenting voices are silenced before they can reach a wide audience ([18]; [19]). Iran's Internet censorship mirrors China's methods in many ways, utilizing privacy-invasive technologies to monitor and suppress political opposition. The use of Deep Packet Inspection (DPI) allows the Iranian government to monitor citizens' online activities and intercept their communications, which is a common tactic used to identify and punish dissidents (Packet, 2012, p. 25).

B. National Security & Crime Prevention

Privacy-invading technologies have become indispensable in the realm of national security and crime prevention as governments seek to protect their citizens from growing threats such as terrorism, cyberattacks, and espionage. Law enforcement agencies use tools like phone tapping, location tracking, and surveillance cameras ([20]) to catch criminals involved in activities ranging from drug trafficking to child exploitation. These technologies, including mass surveillance systems, data collection programs, and cyber monitoring tools, are used to identify and intercept potential dangers before they can manifest. Governments justify their usage as necessary to safeguard society from both domestic and international threats.

For example, in the U.S., surveillance programs such as PRISM, operated by the National Security Agency (NSA), were designed to collect internet data from foreign targets but have also gathered information on U.S. citizens in the process. This presents a delicate balance between ensuring safety and protecting civil liberties, a core challenge in the modern digital age ([21]). The PRISM program has sparked significant debate about the trade-off between privacy and security. While it has been a critical tool for preventing terrorist attacks and protecting national interests, it has raised concerns about the erosion of individual privacy. The exposure of PRISM by Edward Snowden in 2013 highlighted the extent of surveillance conducted by the U.S. government, leading to widespread distrust among citizens ([22]). This conflict has deepened the divide between the government's efforts to maintain security and the public's right to privacy. Many fear that such broad surveillance not only oversteps legal boundaries but also erodes the foundational trust that should exist between citizens and their governments, with long-term implications for democracy and civil liberties ([23]).

Regarding crime prevention, investigators track drug sales and child abuse content sales on the dark web, where anonymity tools like Tor are used by criminals. By analyzing cryptocurrency transactions (often in Bitcoin), investigators can follow the money flow and identify marketplaces or sellers, even though the lifespan of such marketplaces is typically short ([20]).

C. Conflict Between Security and Privacy

Privacy-invading technologies, whether used to consolidate an authoritarian regime's control, protect national security, or prevent crime, ultimately share the same essence: the surveillance of the public. This raises a crucial and complex issue — the conflict between individual privacy and state security. Privacy, a fundamental human right ([24]), is infringed upon when governments monitor their citizens. Surveillance programs, while often justified in the name of safety, are inherently an invasion of personal freedoms.

This creates a vicious cycle. As governments increase surveillance, the public becomes increasingly distrustful and seeks ways to evade such scrutiny, often turning to privacy-enhancing technologies like cryptography. However, this very action triggers further government distrust ([23]). Governments, unable to monitor such activities, respond with legislation or pressure on technology providers to increase surveillance capabilities, further tightening control.

Unfortunately, ordinary citizens lack the power to influence legislative processes, leaving them in a situation where their privacy remains vulnerable. While citizens might be able to shield their data from each other using privacy technologies, they remain transparent to governments and service providers. This imbalance of power means that governments hold all the explanatory authority and can collect personal data at will, leaving individuals without true privacy.

V. The Erosion of Privacy in the Digital Age: A Comprehensive Analysis

A. Examining Privacy in the Digital Age

As society increasingly shifts toward a digital age, individuals are relying more heavily on the Internet to connect with others and using automated processes to simplify daily tasks. To access these services, they must often accept the terms and conditions of the service provider, which involves sharing personal data. However, many users do not thoroughly read these terms, as they feel they have little choice if they wish to use the services. Even those with legal expertise often disregard these terms ([25]).

While these digital services provide convenience and certain protections through PETs against malicious data breaches or unauthorized access, significant risks remain. These include illegal data sharing by corporations and government surveillance, as discussed above. Imagine being constantly monitored — CCTV cameras on every street and in every building, radio frequency identification (RFID) readers tracking every move, vehicles equipped with tracking chips, and phones logging every action Thirty years ago, the idea of being watched 24/7 was dismissed as paranoia; today, it is an undeniable reality. The erosion of privacy extends even to intellectual privacy—the protection of the thought process from external scrutiny—as more of the reading, thinking, and private communications are mediated by electronic technologies (Richards, 2013). The internet has shifted from a realm of anarchic freedom to one of pervasive surveillance and control. While these digital services provide convenience and certain protections through PETs against malicious data breaches or unauthorized access, significant risks remain. These include illegal data sharing by corporations and government surveillance as discussed above. Imagine being constantly monitored — CCTV cameras on every street and in every building, radio frequency identification

(RFID) readers tracking every move, vehicles equipped with tracking chips, and phones logging every action ([26]). Thirty years ago, the idea of being watched 24/7 was dismissed as paranoia; today, it is an undeniable reality. The erosion of privacy extends even to intellectual privacy—the protection of the thought process from external scrutiny—as more of the reading, thinking, and private communications are mediated by electronic technologies ([27]). The internet has shifted from a realm of anarchic freedom to one of pervasive surveillance and control.

VI. The Illusion of Privacy: Government Surveillance, Corporate Data Sharing, and Public Complacency

While all those data may not initially fall into government hands, they often end up there under the guise of laws claiming to serve the public good, protection, and security rather than private interests. Corporations also share data illegally with not only government entities but also other business interests. Notable examples include Facebook's unauthorized sharing of data from 87 million users with Cambridge Analytica and Google's Project Nightingale, which involved secret data-sharing with Ascension, allowing at least 150 employees access to sensitive patient information ([28]).

Despite news of privacy breaches and massive data compromises, many people seem desensitized to them because they may be aware of these breaches, yet there is minimal public response or action to protect digital privacy. Does this indicate that privacy is no longer a top priority for them? Some still argue that people do care about privacy and want to restore their privacy. According to an IAPP report (2023), 68% of online users express concerns about online privacy. In this context, Solove's (2021) suggestion that the framing of privacy-related questions affects people's responses and negative connotations around 'privacy' should be considered, as their actions often tell a different story. Achieving absolute privacy would require complete avoidance of the internet, mobile devices, and IoT technologies. Since people are accustomed to or even dependent on the convenience these technologies offer, they willingly trade privacy for convenience and social conformity ([29]). Thus, the risk to privacy is not only due to companies secretly collecting data but also because individuals actively consent to these risks.

A. The Evolving Concept of Privacy and Its Limitations in the Digital Age

Some people still deny that privacy is dead. They argue that privacy is evolving, defined by the ability to control or manage who sees one's data online ([30]). They point to regulations such as the General Data Protection Regulation (GDPR), which grants individuals more control over their data. However, these measures are more about protecting breached secrets (individual private information) than ensuring absolute privacy. Moreover, they have limited effectiveness; much of the breached data is already in circulation, and digital data is virtually indestructible, as it can be copied or recovered in various ways. For example, former Amazon chief scientist Andreas Weigend once claimed that although the Stasi files on his father were destroyed, the secret police reopened a file on him years later ([31]).

Although PETs, like end-to-end encryption, can prevent service providers from accessing communications between users, they must still provide personal data to opt for these services. Based on evolved definitions, some further suggest that individuals can protect their privacy by avoiding oversharing and managing their data more effectively ([32]). Yet, individual privacy choices can have collective consequences ([33]). Just as a family member infected with COVID-19 can spread the virus if they do not isolate, a breach of one person's privacy can compromise the privacy of others around them. Thus, even if individuals have more control over their online data, collective privacy protection may not be achievable because most people have grown accustomed to or comfortable with sharing their data, often overlooking the risks associated with losing their privacy online.

VII. Conclusion

In conclusion, in this technological era, personal information has become one of the most valuable assets, constantly at risk of being tracked and collected by large institutions for various purposes, such as business and politics. In response to these risks, numerous efforts have been made to protect individual privacy. The development and widespread adoption of Privacy-Enhancing Technologies (PETs) have given users a greater sense of security, as these tools aim to safeguard personal data from misuse and exploitation. However, privacy protection is not solely a technical matter; it also requires the consideration of legal frameworks and regulatory measures, which are often beyond the control of ordinary individuals. It seems that complete privacy is no longer achievable. Instead, a new form of privacy has emerged, where individuals may need to sacrifice some of their personal privacy for broader societal and individual benefits. Nonetheless, it is important to acknowledge that more comprehensive solutions may arise soon as people become increasingly aware of the significance of privacy in the digital age and seek more effective ways to protect it.

References

[1] C. Raab and D. Wright, "Surveillance: Extending the limits of privacy impact assessment," in *Privacy Impact Assessment*, Springer, 2012, pp. 363–383. DOI: 10.1007/978-94-007-2543-0_17.

[2] K. Kan, "Seeking the ideal privacy protection: Strengths and limitations of differential privacy," *Monetary and Economic Studies*, vol. 41, pp. 49–80, 2023.

[3] H. T. Tavani and J. H. Moor, "Privacy protection, control of information, and privacy-enhancing technologies," *ACM SIGCAS Computers and Society*, vol. 31, no. 1, pp. 6–11, 2001. DOI: 10.1145/572277.572278.

[4] Y. Shen and S. Pearson, "Privacy enhancing technologies: A review," Hewlet Packard Development Company, Tech. Rep., 2011.

[5] S. Murthy, A. Abu Bakar, F. Abdul Rahim, and R. Ramli, "A comparative study of data anonymization techniques," in *IEEE BigDataSecurity-HPSC-IDS*, 2019. DOI: 10.1109/BigDataSecurity-HPSC-IDS.2019.00063.

[6] E. Balsa, H. Nissenbaum, and S. Park, "Cryptography, trust and privacy: It's complicated," in *Proceedings of the 2022 Symposium on Computer Science and Law*, 2022. DOI: 10.1145/3511265.3550443.

[7] F. Maqsood, M. Ahmed, M. Mumtaz, and M. Ali, "Cryptography: A comparative analysis for modern techniques," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, 2017. DOI: 10.14569/ijacsa.2017.080659.

[8] G. T. Davies, S. Faller, K. Gellert, *et al.*, "Security analysis of the whatsapp end-to-end encrypted backup protocol," *Cryptology ePrint Archive*, 2023. [Online]. Available: https://ia.cr/2023/843.

[9] E. U. Soykan, L. Karacay, F. Karakoc, and E. Tomur, "A survey and guideline on privacy enhancing technologies for collaborative machine learning," *IEEE Access*, vol. 10, pp. 97 495–97 519, 2022. DOI: 10.1109/access.2022.3204037.

[10] S. Jordan, C. Fontaine, and R. M. Hendricks-Sturrup, "Selecting privacy-enhancing technologies for managing health data use," *Frontiers in Public Health*, vol. 10, Article 814163, 2022. DOI: 10.3389/fpubh.2022.814163.

[11] OSIbeyond, *Printer cybersecurity risks 101*, 2022. [Online]. Available: https://www.osibeyond.com/blog/printer-cyber-security-risks-101/.

[12] P. Radanliev, D. De Roure, M. Van Kleek, and R. M. Montalvo, "Hacking for iot: A brief overview of recent research," *Internet of Things*, vol. 13, p. 100 292, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2667345223000238.

[13] S. M. Bellovin, M. Blaze, S. Clark, and S. Landau, "Going bright: Wiretapping without weakening communications infrastructure," *IEEE Security & Privacy*, vol. 11, no. 1, pp. 62–72, 2012. DOI: 10.1109/msp.2012.138.

[14] Y. Jiang, M. A. R. Baee, L. R. Simpson, *et al.*, "Pervasive user data collection from cyberspace: Privacy concerns and countermeasures," *Cryptography*, vol. 8, no. 1, p. 5, 2024. DOI: 10.3390/cryptography8010005.

[15] CMA Australia, "The dark side of invading social media privacy: Optus data hack," *On Target*, 2022. [Online]. Available: https://ontarget.cmaaustralia.edu.au/optus-data-hack-the-dark-side-of-invading-social-media-privacy/.

[16] T. Dragu and Y. Lupu, "Digital authoritarianism and the future of human rights," *International Organization*, vol. 75, no. 4, pp. 1–27, 2021. DOI: 10.1017/s0020818320000624.

[17] J. Hicks, *Export of digital surveillance technologies from china to developing countries*, 2022. DOI: 10.19088/k4d.2022.123.

[18] S. N. Romaniuk, *China's great firewall and the politics of media control*, 2018. [Online]. Available: https://www.ualberta.ca/en/china-institute/news/the-latest/2018/december/chinas-great-firewall.html.

[19] D. Packet, *The Privacy & Security Research Paper Series*. 2012.

[20] C. Horan and H. Saiedian, "Cyber crime investigation: Landscape, challenges, and future research directions," *Journal of Cybersecurity and Privacy*, vol. 1, no. 4, pp. 580–596, 2021. DOI: 10.3390/jcp1040029.

[21] G. Greenwald and E. MacAskill, *Nsa prism program taps in to user data of apple, google and others*, 2013. [Online]. Available: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[22] A. Florek, "The problems with prism: How a modern definition of privacy necessarily protects privacy interests in digital communications," *The John Marshall Journal of Information Technology & Privacy Law*, vol. 30, no. 3, p. 5, 2014.

[23] T. Jawaid, "Privacy vs national security," *International Journal of Computer Trends and Technology*, vol. 68, no. 7, pp. 1–7, 2020. DOI: 10.14445/22312803/ijctt-v68i7p101.

[24] O. Diggelmann and M. N. Cleis, "How the right to privacy became a human right," *Human Rights Law Review*, vol. 14, no. 3, pp. 441–458, 2014. DOI: 10.1093/hrlr/ngu014.

[25] D. Ibdah, N. Lachtar, S. M. Raparthi, and A. Bacha, "Why should i read the privacy policy, i just need the service: A study on attitudes and perceptions toward privacy policies," *IEEE Access*, vol. 9, pp. 166 465–166 487, 2021. DOI: 10.1109/access.2021.3130086.

[26] D. M. Wood, K. Ball, D. Lyon, *et al.*, *A report on the surveillance society full report*, 2006. [Online]. Available: https://ico.org.uk/media/about-the-ico/documents/1042390/surveillance-society-full-report-2006.pdf.

[27] N. M. Richards, "The dangers of surveillance," *Harv. L. Rev.*, vol. 126, p. 1934, 2013. [Online]. Available: http://ssrn.com/abstract=2239412.

[28] N. Kshetri and J. F. DeFranco, "Is privacy dead?" *IT Professional*, vol. 22, no. 5, pp. 4–12, 2020. DOI: 10.1109/mitp.2020.2992148.

[29] D. J. Solove, "The myth of the privacy paradox," *SSRN Electronic Journal*, 2020. DOI: 10.2139/ssrn.3536265.

[30] R. Ormiston, *Privacy isn't dead; it's just evolving. here's how to keep up*, 2023. [Online]. Available: https://www.osano.com/articles/privacy-isnt-dead.

[31] *Is privacy dead in an online world?* 2017. [Online]. Available: https://www.bbc.com/news/technology-41483723.

[32] R. B. Salem, E. Aïmeur, and H. Hage, "The privacy versus disclosure appetite dilemma: Mitigation by recommendation," in *OHARS@ RecSys*, 2021, pp. 14–32.
[33] C. Veliz, *Privacy is power*. Random House Australia, 2020.