VISUAL REVIEW | Vol. 17, No. 1, 2025 | ISSN 2695-9631
International Visual Culture Review / Revista Internacional de Cultura Visual
https://doi.org/ / .,40/4/-pct tgqs_j,t /7,3769

THE RIGHT TO PRIVACY IN THE DIGITAL AGE: CHALLENGES AND SAFEGUARDS AGAINST MASS SURVEILLANCE FROM A HUMAN RIGHTS PERSPECTIVE

MARÍA FERNANDA MOREIRA MACIAS[1]
[1] Universidad Estatal de Milagro (UNEMI), Ecuador.

PALABRAS CLAVE

Human Rights, Digital privacy, Regulation, Technology, Mass surveillance

RESUMEN

ThThis study analyzes the right to privacy in the digital age from a human rights perspective, addressing the challenges arising from mass surveillance and the guarantees available for its protection. It examines the theoretical, normative, and jurisprudential foundations supporting privacy rights in the digital context, as well as its relationship with other fundamental rights such as freedom of expression and due process. Furthermore, examples of regulatory implementations in different countries and their impact on privacy protection are presented.

Recibido: 03/ 09 / 2024
Aceptado: 25/ 11 / 2024

[1] Lawyer of the Courts and Tribunals of the Republic of Ecuador from Universidad del Pacífico, Escuela de Negocios (UPAC). Master's in Public Administration with a mention in Institutional Development from Universidad Estatal de Milagro (UNEMI). Master's in Human Rights: International Protection Systems from Universidad Internacional de La Rioja (UNIR). Ph.D. candidate in Law at Universidad Católica Santiago de Guayaquil. Professor and Researcher at Universidad Estatal de Milagro (UNEMI).

Email: mbarrenos1@unemi.edu.ec, mercedes.mbs@gmail.com
ORCID ID: https://orcid.org/0000-0002-5912-4476

1. Introduction

Technological developments in recent decades have profoundly transformed the way personal data is collected, stored, and analyzed. The digitalization of multiple processes in areas such as healthcare, education, commerce, finance, and security has enhanced service efficiency but has also raised growing concerns about privacy and the control of personal information. The globalization of technology, driven by the advancement of Big Data, artificial intelligence, the Internet of Things (IoT), and digital platforms, has made data collection an omnipresent practice, where both governments and large corporations access the personal information of millions of individuals without their informed consent and with minimal control over its processing.

Mass surveillance has gained significant prominence in this context, fueling an increasingly intense debate about the limits of this practice and the need to establish effective regulatory mechanisms. While data monitoring can be used to ensure national security, prevent crimes, or improve user experiences across various services, it has also led to numerous abuses that infringe upon fundamental rights. The lack of transparency in data management, the use of biased algorithms, the commercial exploitation of personal information, and the absence of a uniform regulatory framework have contributed to the erosion of the right to privacy and informational self-determination.

From a regulatory perspective, different countries have implemented legal frameworks aimed at protecting citizens' privacy and limiting indiscriminate access to their personal data. Instruments such as the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and Latin American Personal Data Protection Laws have been designed to regulate data access, storage, and processing, establishing rights and obligations for both individuals and entities responsible for data management. However, despite these advancements, legal gaps, differences in protection standards, and the constant evolution of technology continue to present significant challenges to privacy protection.

This study aims to analyze contemporary challenges in personal data protection in the context of mass surveillance. To achieve this, existing national and international regulations will be examined, assessing their effectiveness in defending the right to privacy against new technological dynamics. Additionally, the main risks associated with indiscriminate data collection will be identified, and appropriate protection mechanisms will be proposed to strengthen legal safeguards and enhance citizen control over their own information.

In a world where data has become a highly valuable strategic asset, it is essential to reconsider the balance between technological innovation and respect for fundamental rights. The consolidation of a robust regulatory framework, accompanied by effective oversight mechanisms and increased public awareness of data use and protection, is crucial to ensuring that privacy does not become yet another casualty of technological progress.

2. Theoretical Framework and State of the Art-privacy as a Fundamental Right

Privacy is a fundamental right recognized in various international instruments and national regulations. However, the digital era has posed significant challenges to its protection due to the increased capacity of states and private companies to collect, store, and analyze large volumes of personal information. This section explores the main doctrines, regulations, and theoretical approaches to privacy and its relationship with security in the digital environment.

2.1. International Recognition of the Right to Privacy

Privacy has been safeguarded in various international human rights instruments. The Universal Declaration of Human Rights (UDHR) states in Article 12 that "no one shall be subjected to arbitrary interference with their privacy, family, home, or correspondence, nor to attacks upon their honor or reputation" (United Nations General Assembly, 1948, Art. 12). Similarly, the International Covenant on Civil and Political Rights (ICCPR), in Article 17, protects individuals from any arbitrary or unlawful interference with their privacy, reaffirming the need for effective safeguards (UN, 1966, Art. 17).

At the regional level, the American Convention on Human Rights (ACHR) also recognizes this right in Article 11, ensuring that "no one may be subject to arbitrary or abusive interference with their private life" (IACHR, 1969, Art. 11).

2.2. Doctrines on Privacy in the Digital Age

The digital transformation has led to new interpretations of the right to privacy. Several scholars have argued for the need to reinterpret this right in light of technological advances. Solove (2008) asserts that privacy is not an absolute right but a multidimensional concept requiring a balance between the protection of personal information and the need for data access for legitimate purposes, such as national security and justice administration (p. 62).

On the other hand, Nissenbaum (2010) introduces the concept of "contextual privacy", which suggests that privacy should be assessed based on the context in which data is collected and individuals' expectations regarding their information (p. 89). This approach has been crucial in shaping modern regulations that establish data minimization principles and specific purposes for data collection.

2.3. International Regulations on Privacy and Data Protection

2.3.1. Convention 108 of the Council of Europe

One of the first international legal instruments on data protection is the Council of Europe's Convention 108, adopted in 1981 and updated in 2018. This treaty establishes fundamental principles for the protection of personal data, including legality, proportionality, and transparency in data processing (Council of Europe, 2018, p. 4). The update introduced new provisions reinforcing citizens' control over their data and establishing strict requirements for international data transfers.

2.3.2. General Data Protection Regulation (GDPR) of the European Union

The General Data Protection Regulation (GDPR), adopted in 2016 and in effect since 2018, is one of the most advanced privacy regulations. This regulation establishes key principles for personal data processing, including:

- Lawfulness, fairness, and transparency (Art. 5.1.a)
- Purpose limitation (Art. 5.1.b)
- Data minimization (Art. 5.1.c)
- Accuracy (Art. 5.1.d)
- Storage limitation (Art. 5.1.e)
- Integrity and confidentiality (Art. 5.1.f) (European Parliament & Council of the EU, 2016, p. 12).

The GDPR also grants fundamental rights to citizens, such as the right to be forgotten (Art. 17) and the right to data portability (Art. 20), which allow individuals to request the deletion or transfer of their personal information under specific circumstances (European Parliament & Council of the EU, 2016, p. 27).

2.3.3. Security vs. Privacy in the Digital Age

2.3.3.1. State Surveillance and Mass Data Collection

The dilemma between security and privacy has intensified with the development of mass surveillance technologies. Since the September 11, 2001 attacks, various states have implemented data monitoring and communications surveillance programs under the justification of national security. Programs such as PRISM, revealed by Edward Snowden in 2013, exposed the large-scale access of government agencies to private data (Greenwald, 2014, p. 41).

Some scholars, such as Zuboff (2019), argue that the indiscriminate collection of personal data is not only driven by security needs but also fuels an economic model based on the exploitation of personal information by large corporations (p. 73).

2.3.3.2. The Privacy Debate and Artificial Intelligence

The use of artificial intelligence (AI) algorithms to analyze personal data has raised concerns about the opacity of automated decision-making processes. In many cases, these algorithms may introduce biases that disproportionately affect certain groups, violating principles of fairness and non-discrimination (Binns, 2018, p. 210).

One of the primary challenges in AI regulation is ensuring algorithmic explainability, meaning that automated decisions must be understandable and justifiable. The GDPR introduces the right not to be subject to automated decisions without significant human intervention (Art. 22), providing a legal basis for protecting individuals' rights in the face of AI systems (European Parliament & Council of the EU, 2016, p. 30).

2.4. Protection Mechanisms and Future Challenges

2.4.1. Anonymization and Encryption Tools

The use of data anonymization techniques and end-to-end encryption has been promoted as a solution to protect users' privacy. Tools such as Tor, VPNs, and public-key cryptography help minimize the risk of unauthorized access to information (Schneier, 2015, p. 99).

2.4.2. Regulation of Digital Platforms and Corporate Responsibility

The increasing influence of platforms such as Google, Facebook, and Amazon has led to the need for stricter regulations regarding the collection and use of personal data. The European Union has introduced initiatives such as the Digital Services Act (DSA) and the Digital Markets Act (DMA) to limit the abuses of major tech companies (European Commission, 2022, p. 15).

2.4.3. The Future of Privacy in a Hyperconnected World

The advancement of new technologies, such as quantum computing and the metaverse, raises additional concerns about whether current regulations can adequately protect privacy. It is crucial for legal frameworks to evolve alongside technology to ensure a proper balance between innovation and fundamental rights (Floridi, 2021, p. 56).

The right to privacy faces unprecedented challenges in the digital era. Mass surveillance, the indiscriminate use of personal data, and the development of artificial intelligence require a comprehensive regulatory approach to ensure the protection of fundamental rights. The harmonization of legal frameworks, stronger governmental oversight, and the development of privacy-enhancing technologies will be essential to addressing future challenges in digital privacy and security.

5. Methodology

This study applies a qualitative approach, supported by the analysis of regulations, doctrines, and jurisprudence regarding privacy protection in the digital environment. Three complementary methods are employed to achieve a comprehensive understanding of the phenomenon: the descriptive method, the bibliographic method, and the legal phenomenological method. The application of each of these approaches in the research is detailed below.

5.1. Descriptive Method

The descriptive method is used to analyze the current state of privacy protection in the digital sphere and the application of international regulations on the subject. This method allows for the characterization of the main risks and challenges individuals face regarding mass data collection by governments and corporations.

Through this approach, the study examines key regulatory frameworks such as the General Data Protection Regulation (GDPR) of the European Union, the California Consumer Privacy Act (CCPA), and the Council of Europe's Convention 108, comparing their scope and limitations in defending the right to privacy. Additionally, it identifies technological advancements that have influenced the transformation of personal data protection, including the impact of Big Data, artificial intelligence, and mass surveillance.

The use of this method also facilitates the analysis of landmark cases that have shaped the evolution of privacy law, such as:

- Edward Snowden's revelations about the PRISM surveillance program.
- The sanctions imposed on Facebook over the Cambridge Analytica scandal.
- The controversies surrounding the use of facial recognition systems in public spaces.

5.2. Bibliographic Method

The bibliographic method forms the theoretical foundation of this study, enabling the analysis of relevant doctrinal, regulatory, and jurisprudential sources on privacy protection. A comprehensive literature review is conducted, examining academic research, technical reports, international treaties, and judicial decisions that have set precedents in this field.

Among the primary bibliographic sources considered in this research are:

- Doctrinal works: Texts from authors such as Daniel J. Solove, who explores privacy as a multidimensional concept, and Shoshana Zuboff, who examines the phenomenon of surveillance capitalism.
- International regulations: Analysis of frameworks such as the GDPR, CCPA, Convention 108+, and Latin American data protection laws.
- Relevant jurisprudence: Key rulings from the Inter-American Court of Human Rights (IACHR), the Court of Justice of the European Union (CJEU), and national courts that have interpreted the right to privacy in the digital realm.

The use of this method provides a solid theoretical basis for analyzing contemporary challenges in privacy protection, allowing for a comparison of different doctrinal and regulatory approaches.

5.3. Legal Phenomenological Method

The legal phenomenological method is applied to explore how individuals perceive and experience the loss of privacy in a digitalized world. This approach studies the subjective effects of mass surveillance, data collection without consent, and the use of intrusive technologies in people's daily lives.

This method seeks to answer key questions such as:

- How does digital surveillance affect individuals' perception of privacy and personal freedom?
- What are the most common concerns among citizens regarding the use of their personal data?
- How do data breaches and cyberattacks influence users' trust in digital environments?

To address these questions, the study analyzes reports from international organizations such as the United Nations (UN), the Electronic Frontier Foundation (EFF), and the World Economic Forum, which have conducted research on users' perceptions of privacy and digital security.

Additionally, surveys and public opinion studies from institutions like the Pew Research Center are considered, revealing a growing fear of governmental and corporate control over personal information.

5.4. Justification for the Qualitative Approach

The qualitative approach is appropriate for this study as it allows for a detailed understanding of privacy issues in the digital environment from various normative, doctrinal, and experiential perspectives. Unlike the quantitative approach, which focuses on statistical data analysis, the qualitative approach enables an interpretation of the legal, social, and ethical impact of mass surveillance and personal data collection. The use of three complementary methods ensures a comprehensive analysis of the issue, addressing the evolution of legal frameworks, doctrinal perspectives, and citizens' perceptions of privacy protection.

The methodology adopted in this research enables an in-depth study of privacy in the digital age, considering both existing legal frameworks and the experiences and perceptions of individuals. Through the descriptive method, the current state of personal data protection is examined; using the bibliographic method, the theoretical foundation of the analysis is established; and with the legal phenomenological method, the subjective dimension of the problem is explored. This methodological combination provides a solid framework for understanding challenges and solutions regarding privacy protection in an increasingly digitalized world.

6. Results and discussion

This section analyzes the findings obtained from the study of privacy in the digital context, including its definition, implementation cases and their results, ethical issues, necessary regulations, and relevant case studies.

6.1. Definition of the Right to Privacy

The right to privacy refers to individuals' control over their personal information and how it is used, stored, and shared in both public and private spaces. According to Article 12 of the Universal Declaration of Human Rights (1948) and Article 17 of the International Covenant on Civil and Political Rights (1966), this right ensures protection against arbitrary interferences in individuals' private lives.

In the digital context, this right has evolved to encompass personal data protection, regulating how governments and corporations access, process, and share users' information. Digital privacy has become a central element in contemporary legal and ethical debates, especially with the rise of artificial intelligence, mass surveillance, and data mining.

6.2. Implementation Examples and Results

The regulation of digital privacy has taken different approaches worldwide, with varying results. Below are key examples of regulatory implementations and their impacts:

6.2.1. European Union – General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR), in effect since 2018, has set strict standards for personal data protection. Its main impacts include:

- The obligation for companies to obtain explicit user consent before processing their data (Art. 7).
- The creation of the right to be forgotten, allowing the deletion of personal data under certain conditions (Art. 17).
- The imposition of significant fines on companies violating the regulation, such as the €50 million fine on Google in 2019 by France's National Commission on Informatics and Liberties (CNIL) (European Parliament, 2016, p. 24).

6.2.2. United States – CLOUD Act

In the U.S., the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) allows the government to access data stored on American companies' servers, even if they are located abroad. This raises privacy concerns because:

- It authorizes government agencies to request data without informing the user (Art. 3).
- It exempts companies from complying with foreign data protection laws if they cooperate with U.S. authorities (Art. 5).

The main criticism of the CLOUD Act is that it prioritizes national security over user privacy, creating conflicts with regulations such as the GDPR in Europe.

6.2.3. Ecuador – Organic Law on Personal Data Protection (LOPDP)

Ecuador approved the Organic Law on Personal Data Protection (LOPDP) in 2021, aligning with international privacy standards. Its main advancements include:

- Data minimization principle: Only strictly necessary data may be collected (Art. 8).
- Right to data portability, allowing users to transfer their information between services (Art. 18).
- Administrative sanctions for non-compliance, with fines reaching 1% of a company's annual revenue (Art. 46).

However, its practical application faces challenges, such as a lack of awareness about the regulation among businesses and citizens.

6.3. Ethical Issues in Privacy Protection

The debate on digital privacy involves multiple ethical issues, including:

- Transparency: Companies must be clear about how they collect and use personal data, avoiding deceptive practices.
- Informed consent: Users should control who accesses their data and for what purposes.
- Protection of sensitive data: Information such as biometric, financial, and health data requires stricter security measures.
- Risks of state abuse: Mass surveillance justified in the name of national security may lead to human rights violations, as seen in the NSA's PRISM program.
- Use of artificial intelligence: Automated data processing can reinforce biases and discrimination, affecting credit access, employment, and legal decisions.

6.4. Regulation and Necessary Legal Frameworks

To ensure effective digital privacy protection, national regulations must be harmonized with international standards. Some key proposals include:

- Unifying data protection criteria across countries, promoting regulations equivalent to the GDPR.
- Regulating biometric data collection and storage to prevent misuse in mass surveillance.
- Forcing tech companies to disclose how algorithms influence automated decision-making.
- Ensuring strong oversight and enforcement mechanisms to prevent abuses by both governments and private entities.

The development of a global digital privacy framework is increasingly urgent, given that personal data crosses multiple jurisdictions without effective control.

6.5. Case Studies and International Experiences

To understand the impact of privacy protection (or lack thereof), the following key cases are analyzed:

6.5.1. Cambridge Analytica Scandal (2018)

In 2018, it was revealed that Cambridge Analytica accessed the data of 87 million Facebook users without their consent, using it to influence elections, including Donald Trump's 2016 presidential campaign. This case demonstrated:

- The vulnerability of personal data on social media.
- The lack of regulatory oversight on third-party data usage.
- The need for stricter regulations on the commercial exploitation of personal information.

As a result, Facebook was fined $5 billion by the U.S. Federal Trade Commission (FTC) in 2019.

6.5.2. Surveillance System in China

China has implemented a mass surveillance system integrating facial recognition cameras, data analysis, and a social credit system. Key implications include:

- Citizens cannot avoid constant surveillance.
- Rights restrictions based on social credit scores evaluating "good behavior."
- Severe privacy concerns, as data collection is nearly absolute.

This model poses a significant threat to privacy and has been heavily criticized by human rights organizations.

6.5.3. European Court of Justice Ruling on the 'Right to Be Forgotten'

In 2014, the European Court of Justice recognized the right to be forgotten, allowing individuals to request the removal of personal information from search engines. This ruling established:

- The need to balance the right to information with personal data protection.
- The obligation of companies like Google to handle data removal requests.
- A key precedent in online privacy regulation.

The right to privacy faces growing challenges in the digital era. Although regulations such as the GDPR, Ecuador's LOPDP, and other international frameworks have made significant progress, ethical, legal, and technological issues persist and require comprehensive solutions.

- Mass surveillance, indiscriminate data use, and the lack of user control over personal information demonstrate the urgent need for stronger global privacy protection frameworks.
- Governments and corporations must be held accountable to ensure transparent and ethical data collection practices.
- The development of new regulatory frameworks must address the emerging risks of artificial intelligence, biometric surveillance, and cross-border data transfers.

Privacy is a fundamental right, but without clear and enforceable regulations, it risks being eroded by technological advancements and unchecked surveillance practices. Strengthening international cooperation, regulatory frameworks, and technological safeguards will be essential in preserving digital privacy in the modern world.

7. Ecuadorian regulations on poverty and social protection

In 2021, Ecuador enacted the Organic Law on Personal Data Protection (LOPDP) to guarantee citizens' right to privacy and regulate the processing of personal data in both the public and private sectors. This regulation aligns with international standards, such as the European Union's General Data Protection Regulation (GDPR), establishing fundamental principles governing the handling of personal information.

Among the guiding principles of the LOPDP, the following stand out:

- Principle of lawfulness: Data processing must comply with the law and have the data subject's consent (Art. 8).
- Principle of data minimization: Only the strictly necessary data should be collected for a specific purpose (Art. 11).
- Principle of transparency: Data controllers must clearly inform data subjects about the purpose of collection and the use of their information (Art. 9).
- Principle of proactive responsibility: Entities processing personal data must ensure appropriate security measures and demonstrate compliance with the regulation (Art. 12).

Additionally, the law grants citizens fundamental rights over their personal data, including:

- Right of access: The ability to know what personal data is being processed and for what purpose (Art. 18).
- Right to rectification and deletion: The ability to correct or delete inaccurate or unnecessary information (Art. 19).
- Right to data portability: The ability to transfer personal information between services (Art. 20).

The LOPDP also establishes administrative sanctions for non-compliance, with fines reaching up to 1% of the annual revenue of infringing companies (Art. 46). However, its implementation faces challenges, such as the lack of a data protection culture in public and private institutions and the need to strengthen oversight and enforcement mechanisms.

8. Conclusions

The right to privacy faces new challenges in the digital era, driven by technological advancements, mass data collection, and state and corporate surveillance. Despite the existence of national and international regulations aimed at protecting personal information, legal gaps persist, along with difficulties in the effective enforcement of laws and an increasing power asymmetry between citizens and data-processing entities.

Ecuador has made significant progress in digital privacy regulation with the enactment of the Organic Law on Personal Data Protection (LOPDP), establishing essential principles for protecting personal information. However, its effectiveness will depend on:

1. The implementation of appropriate policies.
2. Active oversight by authorities.
3. Digital education to raise public awareness about privacy rights.

It is crucial to ensure that privacy is protected comprehensively, balancing the need for security and technological development with respect for fundamental rights. To achieve this, it is essential to:

- Strengthen regulatory mechanisms.
- Promote awareness about the importance of data protection.
- Adopt technological tools to mitigate risks associated with mass surveillance.

9. Recommendations

1. Strengthen data protection regulation in Ecuador: Legal reforms and adjustments are necessary to ensure the effective implementation of the Organic Law on Personal Data Protection (LOPDP). Proportional sanctions and efficient enforcement mechanisms must be guaranteed.
2. Implement encryption and anonymization technologies: Encourage the use of tools such as end-to-end encryption, Virtual Private Networks (VPNs),data anonymization techniques. These technologies can reduce data vulnerability and prevent unauthorized access.
3. Promote digital education on privacy and rights: Awareness campaigns should be developed on the importance of online privacy. Citizens, businesses, and public institutions should be educated on responsible data usage and best practices for handling personal information.
4. Establish an autonomous and well-funded data protection authority: The enforcement of the LOPDP should be overseen by an agency with independence from government influence, resources to investigate violations and impose penalties and authority to safeguard privacy rights in Ecuador.
5. Align Ecuador's regulations with international standards: Ecuador should continue adapting its legislation to global frameworks such as the EU's GDPR and OECD recommendations on privacy. Harmonizing regulations would enhance interoperability and ensure adequate protection for citizens.

As digital transformation continues to advance, privacy protection must be a priority. Governments, corporations, and individuals must collaborate to create a secure and fair digital environment, ensuring that privacy rights remain protected in the face of growing technological challenges.

10. Acknowledgments

This study is conducted within the framework of the academic and research commitment of the Universidad Estatal de Milagro (UNEMI), an institution that has been a fundamental pillar in the author's education and professional growth. As a Professor and Researcher at UNEMI, this work reflects the dedication and continuous effort to generate relevant knowledge in the field of human rights, with a particular emphasis on privacy protection in the digital age and the contemporary challenges in defending fundamental freedoms.

I deeply appreciate the support of the UNEMI Directorate of Research and Graduate Studies, as well as the valuable academic exchange with colleagues and students, whose reflections and perspectives have enriched this study. Their contributions have strengthened the analysis of national and international human rights regulations, the evolution of privacy as a fundamental right, and the challenges posed by technology in protecting personal information.

I extend my gratitude to all professionals, researchers, and human rights activists who have shared their knowledge and experiences, providing a deeper insight into current issues and the need to establish effective protection and regulatory mechanisms. Their commitment to defending human dignity and promoting social justice has been a source of inspiration for the development of this study.

References

Binns, R. (2018). Fairness in machine learning: Lessons from political philosophy. *Proceedings of the 2018 Conference on Fairness, Accountability, and Transparency*, 149-159.

Council of Europe. (2018). *Convention 108+ for the protection of individuals with regard to automatic processing of personal data.* Council of Europe.

European Commission. (2022). *Digital Services Act and Digital Markets Act: New rules for online platforms.* European Commission.

European Parliament & Council of the European Union. (2016). *General Data Protection Regulation (GDPR).* Official Journal of the European Union.

Floridi, L. (2021). The ethics of artificial intelligence for a digital society. *Philosophy & Technology, 34(1),* 1-10.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state.* Metropolitan Books.

Inter-American Court of Human Rights. (1969). *American Convention on Human Rights.*

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford University Press.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* W.W. Norton & Company.

Solove, D. J. (2008). *Understanding privacy.* Harvard University Press.

United Nations. (1966). *International Covenant on Civil and Political Rights.* United Nations.

United Nations General Assembly. (1948). *Universal Declaration of Human Rights.* United Nations.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.