BULLET : Jurnal Multidisiplin Ilmu
Volume 1, No. 4, Agustus-September 2022
ISSN 2829-2049 (media online)
Hal 545-552

Sharia-Based Legal Formula For Personal Data Protection In The Financial Services Industry Post-Covid-19 Pandemic

Deny Susanto[1]

[1]Institut Bisnis and Informatics Kwik Kian Gie
deny.susanto@gmail.com

Abstrak−As a country with a substantial Muslim population, Indonesia provides a market for sharia-based financial firms. Corporate organizations, minimal liability companies, seek the most effective way to promote business growth. One objective is to develop its digital ecosystem for the financial services industry, including banking, insurance, capital markets, and non-bank financing organizations. The most crucial factor is the corporation's attempts to deliver effective and efficient services in response to the community's demands as the number of Covid-19 cases continues to fall and the economy begins to improve. This study aims to examine the perspectives on formulating the right and applicable law for the protection of personal data in the management conducted by corporations in the sharia-based financial services sector in Indonesia during the Covid-19 pandemic as post-pandemic expectations. Covid-19 examines law enforcement for potential personal data violations on technology users by businesses. Finding an appropriate and effective legal formulation that can be fundamentally applied in the form of fair regulations and in accordance with sharia values in parallel is the result of the research, and it can be concluded that the formulation of legal rules can rapidly provide regulatory solutions to achieve an equilibrium of rights. and justice for businesses based on sharia law.

Kata Kunci: Personal data protection; corporations; financial services; sharia principles, Covid-19 epidemic

1. INTRODUCTION

Indonesia is a market share for the Islamic finance industry due to the country's majority Muslim population and one of the largest Muslim populations in the world. This plays a significant role for corporations that offer sharia-based financial products as financial service providers. In addition to the high Muslim population, the presence of an Islamic/Sharia economic system is currently viewed as one of the best solutions for reorganizing the Indonesian economy.

With advances in information technology on the one hand and the rise of nationalism and spirituality on the other, we are entering the era of global culture. The period of the "New Economy" (Islamic Economic Concepts) has also left its mark on global culture, and a legal position is increasingly required to regulate it. Sharia Economics is the discipline of those who adhere to the Islamic way of life. Islamic economics examines not only social individuals but also the religious nature of humans. Sharia Economics is governed by fundamental Islamic values derived from the Qur'an and Sunnah.

With the proliferation of Islamic financial institutions (*Lembaga Keuangan Syariah*) such as Bait at Tamwil, Sharia General/Life Insurance, BPRS, and Islamic banking, there is a great deal of public support for the development of Islamic economic practices. People who wish to invest in accordance with sharia-based profit-sharing principles can now do so with confidence through Islamic banking. Islamic banks are governed by the guiding principles of ensuring justice for all parties and contributing to the greater community. Consequently, the bank Shari'ah provisions are implemented by distancing themselves from the element of usury and implementing the profit-sharing principle and the buying-and-selling system (Perwataatmadja & Yeni, 2005).

The term sharia economics is the result of ijtihad in the economic field by Indonesian mujtahids while still referring to the Qur'an, hadith, classical and contemporary literature and taking into account the rapidly and massively developing socioeconomic realities of Indonesian politics and law. This is consistent with the principle that changes in the law are also determined by changes in location and time (*taghayyur alahkam bitaghayur al amkinat wa al-azminat*) (Mahmashani, 1981).

Consequently, the Muslim economy is currently more focused on satisfying consumption needs, making it difficult to allocate funds for investment. In actuality, it is generally accepted that the implementation of Islamic economics in Indonesia today consists primarily of Sharia financial

institutions. In the meantime, the growth and development of Islamic financial institutions are highly reliant on public participation, particularly in the area of fund investment. If the community's investment capacity is weak, it will significantly impact the growth of these Islamic financial institutions.

Along with the growth of human intelligence and reason, the development of civilization continues to accelerate and expand at a rapid rate. In terms of dynamics and contextualization of the role of society, the economic sector is relatively more advanced and faster than the others. The dynamics of human economic life invariably and frequently inform the formulation of legal rules governing it. In this context, Marcus Tullius Cicero, as cited by Isabella Distinto, stated that wherever there are people, there is law, and wherever there is society, there is law (*ubi homo ibi ius, ubi societas ibi ius*) (Distinto, 2013).

The public in Indonesia has recently been surprised by reports in the media regarding the leakage of personal information held by the government or state institutions/agencies as well as private companies in the form of fintech startups.

Regarding the protection of personal data accessible via electronic or digital media, the financial sector in Indonesia requires immediate measures at this time. Personal information stored on electronic or digital media is currently accessible via the Internet as an open system to which anyone may request access with or without security. Personal information can always be linked to other assets, regardless of their monetary worth, so there is a high risk of abuse.

Financial industry participants require the role of the government as a regulator in order to effectively reach the market through digitalization, which is a strategy utilizing digital means.

The digital revolution has created an innovation in the ability to acquire, store, manipulate, and transmit vast and complex volumes of data in real time. Consequently, the digital revolution is frequently equated with the data revolution. No longer relying on considerations of what data might be useful in the future, these advancements have encouraged the collection of various data. Nevertheless, nearly all data has been collected, the government and the private sector are competing to increase their data storage capacity, and data deletion is becoming less common. They find new value in the data and treat it as a tangible asset. This new era of data management is generally known as Big Data (Malik Piyush, 2013).

This shift in the data processing pattern is also referred to as the fourth industrial revolution's core. A digital revolution marked by a convergence of technologies that blurs the distinctions between the physical, digital, and biological fields. The Fourth Industrial Revolution is frequently characterized as the emergence of "cyber-physical systems" with entirely new capabilities for humans and machines, especially in terms of system speed, scope, and impact. These developments have facilitated the emergence of numerous technological advances, including artificial intelligence, robotics, the Internet of Things, automated vehicles, 3D printing, nanotechnology, biotechnology, energy storage, and quantum computing (Schwab, 2017).

Big Data, or the data revolution in general, is frequently regarded as the foundation of technological advancement. This implies that this concept can only be determined by its attributes or elements, comprised of newly discovered data and ultra-advanced computing power. Indeed, the idea of Big Data does not have a definition upon which all experts can agree. However, despite their abundance, there is consensus that Big Data is distinct from traditional business analytics and small-scale data. Due to the breadth of its definition, there are frequently uncertainties and misunderstandings regarding Big Data. The reports are sometimes inconsistent (Ward & Barker, 2013).

From a computer science perspective, Big Data or the data revolution in general is typically viewed as the substance of technological innovation. This implies that this concept can only be determined by its attributes or elements, comprised of newly discovered data and ultra-advanced computing power. As stated by Manovich, Big Data generally refers to sufficiently large data sets (data granularity) that necessitate a supercomputer. Currently, the process can only be analyzed using standard software on a desktop computer (Manovich, 2011).

BULLET : Jurnal Multidisiplin Ilmu
Volume 1, No. 4, Agustus-September 2022
ISSN 2829-2049 (media online)
Hal 545-552

Moreover, Big Data is frequently used to describe the application of analytical techniques to search, collect, and cross-reference large data sets to create intelligence and insight systems. This extensive data collection can be obtained from both public sources and specific customer datasets. Big Data gradually includes not only data of a general nature, but also information gathered by the private sector. This factor then led to the conception of the definition of "Big Data" as the emergence of new data sets with large volumes that change rapidly, are incredibly complex, and surpass the analytical capabilities of hardware and software environments typically used for data processing. In short, the volume of data exceeds the capacity of conventional tools and techniques (Akhgar et al., 2015).

However, several fundamental elements must be considered when utilizing Big Data, particularly those related to privacy and protection of personal data. This refers specifically to a large number of datasets that will facilitate the identification of individuals or groups of individuals who pose a threat to the individual's personal safety. Therefore, appropriate data protection measures must be implemented to prevent data abuse or mismanagement. Strictly speaking, if this massive increase in data collection is not carried out within the context of respecting rights, then it is inevitable that the process and objectives will be used in a way that violates the rights of individuals, namely their privacy.

2. LAW AND DATA PROTECTION

Regarding the rule of law and independence, the law is a moral provision that ensures justice (Grotius, 2005). Grotius, as a humanist, locates the foundation for natural law within the inner human being. Using qualitative and quantitative reasoning, the human capacity for reason can unravel numerous legal mysteries. Humans can analyse the composition of natural laws based on a priori universal principles. Grotius positions natural law as a natural law, similar to positive law in the application.

According to Immanuel Kant, none of the legal authorities are able to define law (noch suchen die juristen eine definition zu ihrem begriffe von recht) (van Apeldoorn, 2001). However, legal definitions continue to be broadly formulated by legal professionals. Twelve legal formulations by Roscoe Pound ranged from ethical-normative to imperative-empirical. In formula number eight, it is stated that the law is a collection of directives from political sovereigns that guide people's conduct(Pound & DeRosa, 2017). According to Qodri Azizy, Roscoe Pound's definition characterizes Roman-era civil law, which later influenced Dutch law and is frequently cited by Indonesian legal scholars (Ismail, 2011) . According to Soeroso and CST Kansil, law is a regulation of human behaviour in social interactions enacted by authorized or authorized official bodies and characterized by its coercive nature, i.e., its ability to command or prohibit, and those who violate it face severe punishments (Kansil & Kansil, 2014; Soeroso, 2002).

According to Plato, law consists of all properly and regularly arranged rules binding judges and society (Hall, 2017). The concept of Plato demonstrates that the law must be codified and binding. Codification is crucial for ensuring the legal certainty of a community. So that society may use it as a reference and behaviour guide. Plato's theory is consistent with John Austin's view that the law is a guideline created by intelligent beings in authority over other intelligent beings (Duxbury, 2005).

As an inherent individual right, the debate over the significance of protecting the right to privacy first arose in British and then American court decisions. Before that, on December 15, 1890, Samuel Warren and Louis Brandeis published a legal conception of the right to privacy in the Harvard Law Review, volume IV, number 5. First to conceptualize the right to privacy as a legal right was the article titled "*The Right to Privacy*" (Warren, 1989). This article first appeared when newspapers began publishing photographs of individuals for the first time. The authors of this paper, Warren and Brandeis, define the right to privacy as "the right to be left alone." Their definition is comprised of two tiers: (i) personal honor, and (ii) values such as individual dignity, autonomy, and personal independence (Bloustein, 1964). This concept was later validated and acknowledged by

the existence of a number of lawsuits that justified the need to protect the right to privacy, especially for moral reasons.

Alan Westin defines the right to privacy as the ability of individuals, groups, and institutions to determine when, how, and to what extent information about them is disclosed to others. The breadth of privacy coverage typically determines the number of privacy-related settings in a country, both in terms of type and level (Westin, 1968). This is similar to the concept proposed by Arthur Miller, which emphasizes the ability of individuals to exercise control over the dissemination of information about themselves in relation to the concept of privacy (Miller, 1975).

From the various definitions of "privacy," it appears that a number of polarizations have emerged, which, in essence, place privacy as an individual's claim, right, or right to determine what information about himself (himself) can be shared with others. Privacy has also been identified as a measure of an individual's control over various aspects of his or her private life, such as I personal information; (ii) the confidentiality of his personal identity; or (iii) parties who have sensory access to the person/personal space (Schoeman, 1984).

In contrast to the United States, which focuses on personal information and communications to define the terms and scope of privacy, the European regime emphasizes the protection of personal data, or simply "data," as part of protecting personal life. This definition refers to Article 8 of the European Convention, which has spawned a number of interpretations regarding the scope of private life, primarily through a number of cases at the European Court of Human Rights (ECtHR) and the European Court of Justice (CJEU). Article 8 of the European Convention defines the scope of personal life as including, among other things, access to personal data, interception of communications, choice or change of name, sexual life, profession or domicile, protection from environmental disturbances, and the right to form and develop relationships with others (Lukács, 2016).

The law governing the protection of personal data actually evolves alongside the advancement of technology, particularly information and communication technology. As stated previously, the data protection regime originated in Europe due to the lack of a clear definition of privacy and private life, which is governed by Article 8 of the European Convention. The right to data protection aims to safeguard individuals in the era of the information society. Germany was the first country to pass the Data Protection Act in 1970, followed by the United Kingdom and a number of other European nations, including Sweden, France, Switzerland, and Austria. 1970 saw the passage of the Fair Credit Reporting Act in the United States, which also contained data protection provisions.

In 2016, the European Union unified its data protection laws through the European Union General Data Protection Regulation (EU GDPR), which went into effect on May 25, 2018. This was a significant development in data protection law. The GDPR is comprehensive, covering nearly all personal data processing. In addition, its implementation will impact not only EU-based data controllers and processors, but also those who offer goods or services to EU citizens or monitor their behavior. As of January 2018, at least 100 countries have adopted data protection laws as national legislation. The scope and scope of data protection, including the scope of data controllers and processors, and territorial/jurisdictional coverage; The definition and types of personal data; Data protection principles, including the justification for data processing; The obligations of data controllers; The rights of the data owner (data subject); and, ordinarily, oversight and enforcement of laws are supplemented by an independent supervisory authority (data protection authority).

In public discourse in Indonesia, the concept of privacy is often identified as a western (European) concept and human rights. This reason justifies the low public awareness of privacy, especially concerning protecting one's personal data. The public in Indonesia quickly tells other people, where they live, their date of birth, and all kinship relationships. In addition, it is also a common practice in Indonesia to submit an identity card (KTP) or other personal identities, in which there is a person's personal data, to a third party, for example when entering a place or building. In the current context, social media users in Indonesia generally openly state their original place of residence (home address); date, month and year of birth; phone number; as well as kinship with

parents or siblings. This shows that there is still a big problem of awareness to protect privacy or personal data, as part of personal property. The claim that privacy is a western concept is actually not entirely valid in Indonesia, a study conducted by Alan Westin (1967), mainly when he provides an overview of the idea of privacy in the pre-modern era or in the structure of traditional society, instead uses the example of household privacy in a social setting. Javanese and Balinese people in Indonesia, with reference to a study conducted by Clifford Geertz. Indeed, as a legal concept of protecting one's privacy, it only came together with the presence of colonial legislation, especially after the ratification of the Civil Code in 1848, and the Criminal Code in 1915, by the Dutch East Indies colonial government. One of these can be identified by the presence of the concept of prohibition to enter other people's houses or yards without permission, or the prohibition to opening a letter without the consent from the Chief Justice, which is regulated in Postordonnantie 1935 (Staatsblad 1934 No. 720).

The right to privacy, including the protection of personal data, was recognized as one of the citizens' constitutional rights during its development, particularly after the 1945 Constitution was amended. This is the case in accordance with the inclusion of a particular chapter on human rights (bill of rights) in the amended constitution (Chapter XA—Article 28 A-J). Article 28G paragraph (1) of the 1945 Constitution contains provisions regarding the guarantee of the protection of personal data; it states, "Everyone has the right to protection for personal protection, family, honour, dignity, and property under his control, and is entitled to a sense of security and protection from the threat of fear to do or not do something, which is a human right." In addition to constitutional protection, Indonesia's participation as a state party to the International Covenant on Civil and Political Rights (ICCPR), which was ratified by Law No.12/2005, affirms the government's duty to protect privacy and personal data of its citizens.

This is also consistent with Law No. 39/1999 on Human Rights, which guarantees the protection of citizens' right to privacy in multiple articles, including Article 14.2, Article 29.1, and Article 31. Article 29, paragraph 1 generally recognizes the rights of all individuals to the protection of their personal, family, honour, dignity, and property rights. This protection extends not only to direct relationships, but also to personal information or data. Article 14 paragraph 2 states that one of the rights to self-development is the right to seek, obtain, store, process, and transmit information using any and all available means; and while it is true that this right is a component of the right to self-development, it is not a fundamental right. This relates to Article 31 of the Human Rights Law, which also guarantees the confidentiality of electronic communication unless compelled to do so by a court order or other lawful authority.

On a more granular level, there are also a number of laws and regulations in effect that relate to or contain information about personal data—protection, collection, processing, use, and disclosure. Several of these laws and regulations can be classified according to the following sectors: (i) telecommunications and informatics; (ii) population and archives; (iii) **finance, banking, and taxation**; (iv) trade and industry; (v) health services; and (vi) security and law enforcement.

3. INDONESIA'S DATA PROTECTION PRACTICES

The Institute for Community Studies and Advocacy—ELSAM (Kontan, 2019) found a number of discrepancies between the privacy policies and terms of service of 10 information and communication technology-based companies in Indonesia and the principles of personal data protection. Some companies from outside Indonesia have attempted to at least comply with the EU GDPR data regulations, while a number of Indonesian companies have not adopted any personal data protection policies at all. In addition to a lack of understanding of privacy and consumer data protection, the absence of the Personal Data Protection Law is the primary reason why they do not comply with data protection regulations. According to the Minister of Communication and Information, Rudiantara, the process of debating the Personal Data Protection Bill must be accelerated so that Indonesian e-commerce can also develop its market in countries that require personal data protection in trade relations.

The Banking Law (Law No.10/1998) governs, among other things, bank secrecy (Husein, 2010), which is based on the confidentiality principle, which requires banks to keep all data and information about customers, including financial and personal information. Bank secrecy is defined in Article 1 paragraph (28) of the Banking Law as "*all information concerning depositors and their deposits*"(Gazali & Usman, 2012). Thus, the principles of trust and confidentiality that underpin financial institutions performance are also applied in the customer-bank relationship. Customers who make deposits or use other bank products must provide the bank with personal information that is deemed necessary.

This relationship must be supported by the bank's ability to maintain customer trust while also protecting the privacy of customers who have provided and entrusted personal data to the bank. This is stated in Article 40 of the Banking Law and Article 41 of Law No. 21/2008 concerning Islamic Banking, which state that banks are required to keep information about their depositors and deposits confidential, except in limited circumstances. The regulation implies that customer privacy is protected not only in relation to their financial data (savings or other bank products), but also in relation to the customer's personal data that is informational or information relating to identity or other personal data other than financial data.

With the passage of Law No. 21/2011, the Financial Services Authority was established, with supervisory authority over all financial service providers, including banking, which was previously supervised by the central bank. This includes ensuring the confidentiality of customers' personal information. This provision was later reaffirmed by OJK Regulation (POJK) No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, which emphasizes in point Article 2 letter (d) that the basic consumer protection principles that OJK must follow are based on the principles of confidentiality and security of consumer data/information. In fact, this POJK includes a special chapter that governs consumer protection oversight in the financial services sector, which is entirely under the authority of the OJK.

OJK even contains a more detailed list of consumer personal data and/or information that must be kept confidential through OJK Circular Letter Number 14/SEOJK.07/2014 concerning Confidentiality and Security of Consumer Personal Data and/or Information, in the form of name, address, telephone number, date birth and/or age, and/or biological mother's name (specifically for individual customers), as well as the composition of the board of directors and commissioners including identity documents in the form of Identity Card/passport/residence permit, and/or composition of shareholders (especially for corporate customers). In addition, responding to the development of financial technology services, which are also accompanied by the practice of collecting personal data of consumers, OJK has also issued two regulations: (i) POJK No.77/POJK.01/2016 concerning Information Technology-Based Lending and Borrowing Services (LPMUBTI); and (ii) POJK No.13/POJK.01/2018 concerning Digital Financial Innovation in the Financial Services Sector.

At the 2017 G20 meeting in Hamburg, G20 ministers agreed on the significance of protecting personal data in the context of the growth of the digital economy. This agreement was subsequently revealed in the E-Commerce Roadmap, which was ratified by Presidential Regulation No.74/2017 regarding the Roadmap of the National Electronic-Based Trading System for 2017-2019. According to this Presidential Regulation, the development of e-commerce in Indonesia has eight priorities, including funding, taxation, consumer protection, education and human resources, communication infrastructure, logistics, cyber security, and the establishment of management for the 2017-2019 SPNBE implementation. The discussion of the protection of personal data is one of the consumer protection's top priorities.

In fact, in response to the aforementioned needs, a number of other ASEAN nations have already begun to develop special rules for the protection of personal data. Singapore in 2012, Malaysia in 2010, the Philippines in 2012, Laos in 2017, and Thailand in 2019 are some examples. Indonesia's participation in a number of trade agreement negotiations, including the PTA, RCEP, and CEPA, which have recently begun to discuss the e-commerce sector and the issue of cross-border data flows, necessitates an immediate improvement in the country's data protection regulations. Not to mention the enforcement of the EU General Data Protection Regulation (GDPR)

on May 25, 2018, which has had a significant impact on Indonesian companies in various sectors, including transportation, e-commerce, hospitality, and other industries that collect personal data.

In general, the public does not view personal data as property that must be protected. This can be inferred, among other things, from the number of posts on social media platforms and in social networking groups that contain personal data. In addition, when utilizing a variety of electronic system platforms (e-commerce, online transportation, fintech, etc.), users do not fully comprehend the privacy policies and terms and conditions of service of each of these applications, particularly those pertaining to the use of personal data.

In response, a more instrumental and structural approach, including the establishment of a comprehensive personal data protection law, is required. This strategy is also consistent with a number of actual trends that are closely related to the practice of collecting personal information by government and private institutions.

4. CONCLUSION

Future issues must be anticipated especially after the pandemic Covid-19, particularly with the growth of digital transactions in the Islamic finance industry, which employs product marketing strategies via a variety of application platforms, including web and smartphone applications.

Indonesia does not yet have a specific regulation regarding the Protection of Personal Data and/or Digital Assets; therefore, a regulation regarding Personal Data Protection, particularly in the insurance industry, is essential. Electronic/Digital Personal Data Protection is not only from a technological perspective, but also from a legal perspective, so that the security of electronic data can be protected by law. Personal Data Protection is always associated with digital assets; consequently, laws and regulations pertaining to digital assets are also required, particularly with regard to the portfolios or asset profiles of parties interested in Islamic financial services.

In order for the Islamic financial services industry to grow positively and be able to provide the best service performance for the user community, and for the user community to also feel that they are receiving the best service performance, the Islamic financial services industry requires urgent government support, particularly from ministries concerned with the protection of digital aspects and the Financial Services Authority as a supervisor.

REFERENCES

Akhgar, B., Saathoff, G. B., Arabnia, H. R., Hill, R., Staniforth, A., & Bayerl, S. (2015). *Application of big data for national security: a practitioner's guide to emerging technologies*. Butterworth-Heinemann.
Bloustein, E. J. (1964). Privacy as an aspect of human dignity: An answer to Dean Prosser. *NYUL Rev.*, *39*, 962.
Distinto, I. (2013). *Legal Ontologies for Public Procurement Management*.
Duxbury, N. (2005). English jurisprudence between Austin and Hart. *Va. L. Rev.*, *91*, 1.
Gazali, D. S., & Usman, R. (2012). Hukum Perbankan. *Jakarta: Sinar Grafika*, *271*.
Grotius, H. (2005). *Stanford Encyclopedia of Philosophy*.
Hall, J. (2017). Plato's legal philosophy. In *Plato and Modern Law* (pp. 33–68). Routledge.
Husein, Y. (2010). *Rahasia Bank dan Penegakan Hukum*. Pustaka Juanda Tigalima.
Ismail, G. (2011). *Eklektisisme Hukum Islam dan Hukum Umum: Upaya Menuju Kelahiran Hukum Nasional*.
Kansil, C. S. T., & Kansil, C. S. T. (2014). *Pengantar ilmu hukum Indonesia*.
Kontan. (2019, March 19). *Industri e-commerce terganggu bila RUU perlindungan data pribadi belum rampung*.
Lukács, A. (2016). *What is privacy? The history and definition of privacy*.
Mahmashani, S. (1981). Falsafah al-Tasyri'fi al-Islam, terj. *Ahmad Sujono. Bandung: Al-Ma'arif*.
Malik Piyush. (2013). *Governing Big Data: Principles and practices: Vol. 57 (3/4)*. IBM Journal of Research and Development.
Manovich. (2011). *Trending: The promises and the challenges of big social data. Debates in the digital humanities* (Vol. 2).
Miller, A. A. (1975). The assault on privacy. *Psychiatric Opinion*.
Perwataatmadja, K., & Yeni, G. (2005). Bank dan asuransi Islam di Indonesia. *Jakarta: Kencana*.
Pound, R., & DeRosa, M. L. (2017). *An introduction to the philosophy of law*. Routledge.
Schoeman, F. (1984). Privacy: philosophical dimensions. *American Philosophical Quarterly*, *21*(3), 199–213.

Schwab, K. (2017). *The fourth industrial revolution*. Currency.
Soeroso, R. (2002). *Pengantar ilmu hukum*.
van Apeldoorn, L. J. (2001). *Pengantar ilmu hukum (Inleiding tot de studie van het Nederlandse recht)*.
Ward, J. S., & Barker, A. (2013). Undefined by data: a survey of big data definitions. *ArXiv Preprint ArXiv:1309.5821*.
Warren, S. and L. B. (1989). *The right to privacy." In Killing the Messenger*. Columbia University Press.
Westin, A. F. (1968). Privacy and freedom. *Washington and Lee Law Review*, *25*(1), 166.