# SOCIO-POLITICAL INFLUENCES ON DATA PRIVACY AND SECURITY

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science, School of Engineering

**Kevin Bruzon**

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Pedro A. P. Francisco, Department of Engineering and Society

# SOCIO-POLITICAL INFLUENCES ON DATA PRIVACY AND SECURITY

## Introduction

The digital age has served as a platform for unprecedented technological growth and developments. However, this unprecedented growth is yielding more room for data privacy threats. In recent years, technology has become increasingly intertwined with society and everyday life, resulting in more data being stored on the internet. With this technological growth, public concern regarding data privacy has grown in parallel. In order to protect individuals from privacy threats, many governments around the world have implemented data privacy legislation. Data privacy legislation provides a legal framework on the collection, use, and storage of personal data. This legislation is designed to ensure that personal data is not used or shared without the permission of individuals or companies. It also requires organizations to have adequate security measures in place to ensure the security and protection of data. In light of the growth of data collection and use by companies and the potential risks associated with it, the effectiveness of data privacy legislation is often questioned, with many nations implementing weak legal frameworks that fail to adequately address public concerns regarding the privacy and security of personal data. Even worse, some data privacy legislations have begun to loosen access restrictions, allowing for data access to be granted to government groups and law enforcement agencies. Different socio-political contexts are driving data privacy legislation into a state of weakness and ineffectiveness, yielding more room for threats and concern.

It is essential to examine data privacy legislation on a global scale in order to gain an understanding of how socio-political contexts can work to positively reinforce data privacy legislation, that is strong, effective, and protective of data. Technology is rapidly growing and evolving, resulting in more data being at risk as time goes on. The public is not fully aware of

this, let alone the state of their legal frameworks to protect personal data. It is also important to shed light on the growth of data privacy concerns and threats, the importance of legislation as a device for protection, as well as the methodologies and processes of strong, effective, and protective data privacy legislation.

**Methodology**

This research will analyze the role of socio-political contexts in shaping data privacy legislation in various nations, seeking to answer the question: how do socio-political contexts shape and influence data privacy legislation? The aim is to gain insights on the contexts that influence legislation, and in turn, explore crucial methodologies for the implementation of effective legislation. Applying these methodologies in data privacy legislation would promote positive reinforcement from socio-political contexts, while addressing the concerns of the public, yielding effective data privacy protections.

Sources such as journal articles, research papers, and legal documents were used, from which a literature review is conducted. In these various sources, there are three key components that will be gathered from research. The first is the situation or problem at hand regarding data privacy discussed in the source. The second is the current social and political contexts of influence in the setting discussed in the source. The third is identifying all the relevant social and political groups as well as their relationships with data privacy legislation. Next, these three components are tied together under the same lens in order to gain a better understanding of the current state of legislation. Afterwards, data privacy legislation is broken down into two categories: weak legislation or strong legislation. Legislation failing to address the concerns or needs of a relevant social or political group or receiving unbalanced influence from the relevant groups will be categorized as weak. On the other hand, legislation addressing the needs of all

relevant groups and preserving a balance of influence amongst groups will be categorized as strong legislation.

A theoretical analysis is also performed, which applies the Social Construction of Technology (SCOT) theoretical framework, originally introduced in 1984 by Trevor Pinch and Wiebe Bijker. Although this framework is geared towards a technical subject, it is adapted to a non-technical subject, data privacy legislation. This adaptation is a result of the framework being very effective at depicting and outlining the relationships between the subject and relevant social and political groups/contexts, aiding in presenting a visualization of how the contexts influence data privacy legislation. Following the application of the framework, methodologies for improving and yielding effective legislation are discussed.

This research is presented with the desired outcome being greater public awareness and responsiveness to privacy concerns and threats. Furthermore, it is important for governments, technology companies, and the public to consider the influence of socio-political contexts in order to ensure data privacy legislation is implemented to effectively protect personal data.

**Literature Review**

According to Vernon Andrews, a bachelor of cybersecurity from Columbus State University, today's methods of data storage on the internet have resulted in an emergence of concerns and issues pertaining to data privacy (2019). Furthermore, according to Yang, a researcher at the University of Melbourne and Xu, and Xu, a senior lecturer in communication at Deakins University, privacy issues have been an ongoing debate in the United States since the Internet was first made public (2018). Andrews also reveals, from the results of a questionnaire, that society has a lack of knowledge regarding data privacy issues (2019). The rapid growth of

technology has spurred a need for research regarding data privacy issues, which much of the public is not yet aware of. Even worse, various nations have begun opening the doors for access of private data with loosened restrictions in their legal frameworks. To tackle these issues, governments and nations must prioritize the implementation of strong legal frameworks designed to protect against personal data access, while taking into account the public's concerns and socio-political contexts.

The California Consumer Privacy Act in the United States is exemplary of strong data privacy legislation. The California Consumer Privacy Act (CCPA) is a comprehensive privacy law that was enacted in 2018 and went into effect on January 1, 2020. It provides California residents with more control over their personal information and data. The CCPA gives California residents the right to know what personal information a business has collected about them, the right to delete their personal information, the right to opt-out of the sale of their personal information, and the right to be free from discrimination for exercising their rights. The law also requires businesses to provide clear notice about what data is being collected, how it's being used, and who it's shared with. Additionally, the CCPA grants the California Attorney General the power to enforce the law, and provides for civil penalties for non-compliance (Kaminski et al., 2020).

Another great example exists in Canada. The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian federal law that sets out the ground rules for how private sector organizations may collect, use, and disclose personal information in the course of commercial business. The law also provides individuals with a right to access the personal information that organizations hold about them. PIPEDA applies to all private-sector organizations in Canada, including businesses, charities, and not-for-profit organizations. The

law sets out the principles for how organizations must handle personal information in order to protect the privacy of individuals. These principles include obtaining consent for collecting, using, or disclosing personal information, limiting the collection of personal information to what is necessary for the purposes identified, and ensuring that personal information is accurate and securely stored. PIPEDA also requires organizations to inform individuals about their privacy practices and provide individuals with access to their personal information upon request. Organizations must also have policies and procedures in place to protect personal information from unauthorized access or disclosure. The law also includes provisions to ensure that personal information is not transferred to countries that do not have similar privacy laws. Organizations must obtain consent before transferring personal information to a third party, and must ensure that the third party provides an adequate level of protection for the personal information (Office of the Privacy Commissioner of Canada, 2021).

Many weak legal frameworks are currently in place around the world, failing to ensure the protection and security of private data, not addressing the concerns of the public, and receiving an unbalanced influence from relevant social and political groups. In China, the emergence of technology embedded in urban development has driven the public to raise privacy concerns as a result of weak legal frameworks for data privacy protection (Yang & Xu, 2018). Firstly, there exists a grave issue with China's cyberspace regulatory framework, which is largely seen as restrictive and often in conflict with internationally accepted principles of freedom of expression. The framework has had a negative effect on innovation, economic growth, and international collaboration (Kshetri, 2014). Secondly, a huge weakness in the legal development of data protection in China is that the current legal protection remains weak. There is a lack of a comprehensive data protection law and the existing rules are scattered within various types of

law. In addition, the Cybersecurity Law does not adequately address data protection issues, leaving China behind global trends in this area. Another major weakness is that the thresholds for criminalizing data abuse are too low, resulting in a lack of enforcement of punitive provisions in criminal law. Additionally, due to a lack of resources, enforcement agencies often only investigate and prosecute cases involving a large number of pieces of personal data, leaving many less serious but criminally punishable cases unpunished. (Feng, 2019).

Meanwhile in Australia, due to criminal acts and terrorism, the government issued legislation which grants law enforcement agencies access to "an unlimited range of technical assistance, extending beyond decryption to include modifying consumer products and services" (Hardy, 2020, para. 3). Furthermore, Australia's Privacy Act 1988 Australia's information privacy law is limited in scope, not up to date with other international standards, and has weak sanctions and penalties. It also does not provide additional rights to protect privacy in the context of Big Data or similar technologies, and has open data policies with insufficient regard for the limitations of de-identification techniques. In addition, the mandatory data breach notification laws only apply to certain sectors and do not require those affected to be notified within a reasonable time. Furthermore, Australia has enacted far-reaching anti-terrorism and national security laws that allow law enforcement and national security agencies to access metadata without warrant and exempt from privacy laws. At a state and territory level, public sector privacy protection has been weakened by recent legislative amendments that mandate information sharing between government agencies and provide for personal information to be made available to government-appointed chief data officers (Watts & Casanovas, 2019).

Similarly, many European nations have joined the debate of granting access to private encrypted data due to crime and terrorism. (Severson, 2017). Furthermore, according to

Severson, a Harvard Law School graduate, in France there is legislation in place that grants law enforcement agencies technical assistance in gathering information during criminal investigations (2017). Rather than ensuring the protection and security of data, many data privacy legislations are being driven to granting access to government groups and law enforcement agencies by their respective socio-political contexts, not addressing the concerns of the public as well as limiting their rights, and ineffectively regulating measures of legislation. This, along with increasing prevalence of technology and internet in everyday lives, has resulted in a serious problem: with more and more personal data is being stored online, there is increased room for data privacy concerns and threats.

Bart Jacobs, a Dutch computer scientist and professor of security, privacy and identity at Radboud University, and Jean Popma, a Dutch cybersecurity expert and project manager for applied security research at Radboud University, offer some suggestions for effective data privacy and security that can aid these weak legal frameworks. In 2019, in their article “Big Data and the need for privacy by design”, Jacobs and Popma discuss their involvement with a Parkinson’s research project, in which they implemented a secure and private data management system. Although written in the context of medical research, they determine four processes that are essential to effectively preserve data privacy: “informed consent, data governance, data use agreements and data security” (2019). The first process, informed consent, consists of a participant approving they are aware of the risks, the purpose of the study, as well as how data will be used. The second process, data governance, embodies the organizational aspect of data typically consisting of a board of relevant stakeholders, and an authoritative figure. The third process, data use agreements, embodies the legal aspect of data and presents the groundwork for data governance. The obligations, rules, and regulations pertaining to the sharing of data are

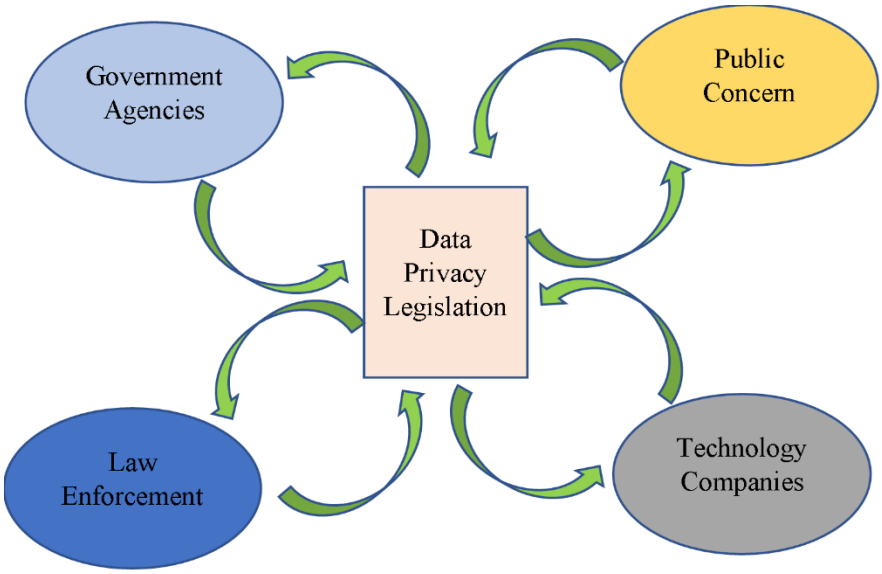
outlined in data use agreements, and data governance bodies cannot exercise any actions pertaining to the data without them. The fourth process, data security, consists of the implementation of secure and private methods for data sharing. Ultimately, Jacobs and Popma conclude that in order to ensure security and privacy when sharing data, a multidisciplinary professional approach is crucial.

**Discussion and Results**

By conducting an in-depth analysis of the data privacy legislations in different countries, this research aims to uncover any potential issues or gaps in the legislations, as well as the various contexts, processes and methodologies that have gone into their formulation. To achieve this, the Social Construction of Technology (SCOT) framework, first developed by Trevor Pinch and Wiebe Bijker in 1984, will be used. Figure 1 depicts this framework in the context of strong data privacy legislation, outlining the balanced positive relationships between data privacy legislation and the different socio-political contexts and groups that shape data privacy legislation, as well as the protection of data privacy.

**Figure 1**

*Strong Data Privacy legislation SCOT model*



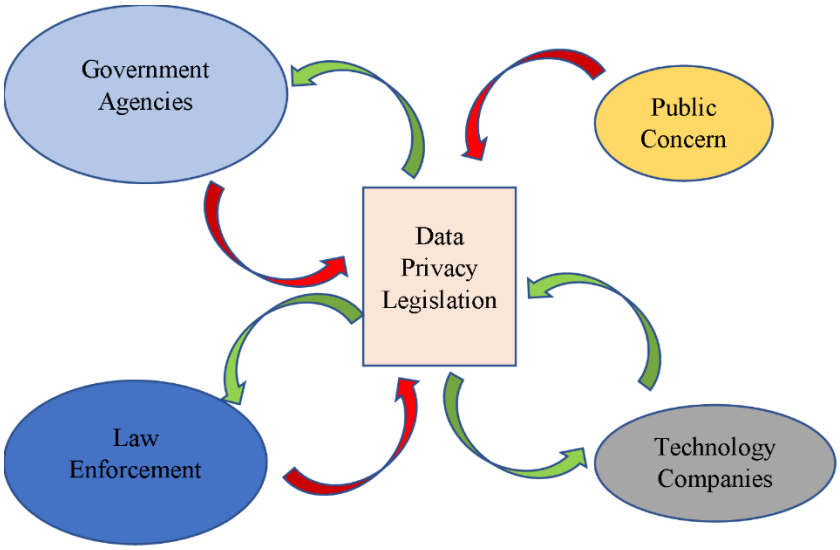

*Note*: This figure depicts the application of the SCOT framework, outlining the different social and political groups that shape strong data privacy legislation. A positive relationship between the groups and data privacy legislation is outlined by the green color in the arrows, and the size of the shapes depicts a balanced influence across all the groups. (Adapted by Bruzon (2022) from Carlson, 2009)

Strong data privacy legislation is shaped by many different groups, such as the government, law enforcement agencies, technology companies, and the public. These groups are influenced by the social and political contexts in which they operate, but in turn, data privacy legislation also has an impact on them and the contexts in which they exist. The CCPA, a strong legislation, grants California residents (the public) the right to know what personal information a business has collected about them, the right to delete their personal information, the right to opt-out of the sale of their personal information, and the right to be free from discrimination for exercising these rights. This can be noted in Figure 1, where the public positively reinforces the implementation of legislation, while modifications and improvements to the legislation presents the public with

the opportunity to have a more positive and active role in making decisions relevant to personal data. Furthermore, California Attorney General has the power to enforce the legislation, and provides civil penalties for non-compliance. This is evident in Figure 1, where government agencies are also depicted to have a positive influence on legislation, helping shape it and enforce it, while legislation provides the government agencies with a just framework to enforce. Also, PIPEDA establishes guidelines for private-sector organizations in Canada on how they must handle personal information in order to safeguard the privacy rights of individuals. This includes businesses, charities, and not-for-profit organizations. This can be noted in Figure 1, where private-sector companies such as Technology Companies are influenced by legislation, being provided with guidelines to follow to ensure data privacy is enforce and preserved. In turn these companies establish and developed measures and procedures for security and protection that can contribute to the implementation, as well as provisions of legislation. Finally, the enforcement powers for both the CCPA and PIPEDA lie in the hands of the government agencies, with law enforcement agencies having no power to enforce the provisions of legislation; however, law enforcement agencies such as police departments are granted limited rights to dealing with secure and private data, with more lenient rights being granted in terms of criminal cases or matters of national security. This is evident in Figure 1, where there exists a positive relationship between law enforcement agencies and legislation. Legislation provides law enforcement agencies with a balanced set of powers when dealing with personal data, while law enforcement agencies positively enforce and preserve the provisions of legislation, ensuring that data privacy is protected. Overall, Figure 1 depicts balanced and equal relationships of influence among all relevant social and political groups, revealing how comprehension amongst relevant groups is essential for the implementation of strong and protective legislation.

**Figure 2**

*Weak Data Privacy legislation SCOT model.*




*Note*: This figure depicts the application of the SCOT framework, outlining the different social and political groups that shape weak data privacy legislation. A negative relationship between the groups and data privacy legislation is outlined by the reed color in the arrows, and the size of the shapes depicts an imbalanced influence across all the groups. (Adapted by Bruzon (2022) from Carlson, 2009)

Figure 2 serves as a juxtaposition, and depicts the SCOT framework in the context of weak data privacy legislation, outlining the relationships between data privacy legislation, and the different socio-political contexts and groups that shape data privacy. It outlines how weak data privacy legislation often fails to adequately preserve data privacy due to incomplete relationships between all relevant parties and contexts. Without comprehensive coverage of all stakeholders and contexts, data privacy laws can have unintended negative consequences, such as opening the door to increased access to private data. In China, the restrictive legal frameworks and the lack of alignment with international standards of freedom of expression are major issues that are indicative of weak legislation. This is depicted in Figure 2, where public concern is depicted with

only one arrow, with the legislation negatively influencing the public, restricting their rights pertinent to their personal and private data, rather than positively impacting the public and granting them more rights. In Australia, anti-terrorism and national security laws allow law enforcement and national security agencies to access metadata without a warrant, while being exempt from privacy laws. In China, due to a scarcity of resources, law enforcement agencies primarily focus on cases involving a substantial amount of personal data, thereby allowing smaller, yet still punishable, cases to go uninvestigated and unpunished. This can be seen in Figure 2, where law enforcement agencies negatively impact legislation, not fully enforcing the established provisions as well as not preserving data privacy protections for all relevant groups, as they let smaller instances of violations slip by. On the other hand, legislation positively impacts the law enforcement agencies, granting them access rights to carry out investigations without having to abide by the legislation. Similarly, in Australia, recent legislative amendments have weakened privacy protection in the public sector by mandating the sharing of information between government agencies and allowing for personal data to be accessed by government-appointed chief data officers. This is evident in Figure 2, where government enforcement agencies negatively influence legislation, shaping it to be loose and less protective, while the legislation positively impacts the government agencies as it ultimately grants them extensive data access in order to carry out their agendas, without having to abide by the provisions of the legislation. Finally, in Australia, the current legislation is very outdated, with minimal updates to the provisions. It has presented private-sector organizations such as technology companies with very easy rules and regulations to abide by, keeping them happy and able to operate and make developments without violating data privacy laws. Furthermore, the technology companies are still preserving the data privacy legislation and reinforcing the current implemented framework

as it satisfies their agendas. This is depicted in Figure 2, where a positive relationship exists both ways between legislation and technology companies. Ultimately, the key component that is evident in weak legislative frameworks is revealed in Figure 2 as a lack of balance and comprehension amongst the relevant social and political groups. In order to yield an improvement in data privacy protection, it is essential for these socio-political groups to consider the four processes discussed by Bart Jacobs and Jean Popma. In particular, the implementation of data governance would yield much more effective protections for data. These weak legal frameworks currently leave all the governance to government and law enforcement agencies, failing to include all relevant stakeholders, in particular, the public. It is essential that these frameworks develop a sense of governance and create a balance of influence among all stakeholders. Furthermore, this balance must be achieved through a a multidisciplinary network of stakeholders.

**Conclusion**

Technology has revolutionized society with its ability to make everyday life easier, however, with this progress come risks to data privacy. As the advances, growth, and increased embeddedness of technology become more prevalent in society, it has become increasingly important to be aware of the implications it may pose to data privacy. To ensure that data privacy is safeguarded, nations across the world have implemented data privacy legislation intended to protect data and mitigate concern. Although this legislation is a major step forward, there have been varying levels of success in its application and implementation. Therefore, data privacy legislation must be employed as a tool to counter the risks posed by technological advances, utilizing the collective expertise and influence of various socio-political contexts to ensure that data privacy is safeguarded in the future.

## References

Andrews, V. (2019) Analyzing awareness on Data Privacy. *Proceedings of the 2019 ACM Southeast Conference* (pp. 198-201). Association for Computing Machinery. https://doi-org.proxy01.its.virginia.edu/10.1145/3299815.3314458

Bijker, W. E., & Pinch, T. J. (1984). The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, 14(3), 399–441. https://doi.org/10.1177/030631284014003004

Bruzon, K. (2022). Strong Data Privacy legislation SCOT model. [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Bruzon, K. (2022). Weak Data Privacy legislation SCOT model. [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Carlson, B. (2009). [SCOT figure description and example]. *Class handout* (Unpublished). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Hardy, K. (2020). Australia's encryption laws: practical need or political strategy? *INTERNET POLICY REVIEW*, 9(3, SI). doi:10.14763/2020.3.1493

Jacobs, B., & Popma, J. (2019, January). Medical research, Big Data and the need for privacy by design. *Big Data & Society*, 6(1), 205395171882435. https://doi.org/10.1177/2053951718824352

Kaminski, M., Snow, J., Wu, F., & Hughes, J. (2020). Symposium: The California Consumer Privacy Act. *Loy. L.A. L. Rev.,* 54(157). Retrieved March 15, 2023, from https://digitalcommons.lmu.edu/llr/vol54/iss1/3/

Kshetri, Nir (2014). "China's Data Privacy Regulations: A Tricky Trade-Off between ICT's Productive Utilization and Cyber-Control", , 12(4), 38-45.

Office of the Privacy Commissioner of Canada. (2021, December 8). The Personal Information Protection and Electronic Documents Act (PIPEDA). *Office of the Privacy Commissioner of Canada.* Retrieved March 15, 2023, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Severson, D. (2017). The encryption debate in Europe. *Hoover Institution Aegis Paper Series*, (1702).

Watts, D., & Casanovas, P. (2019, June 27). Privacy and data protection in Australia: a critical overview (extended abstract). w3. Retrieved March 15, 2023, from https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf

Yang Feng (2019) The future of China's personal data protection law: challenges and prospects, *Asia Pacific Law Review*, 27:1, 62-82, DOI: 10.1080/10192557.2019.1646015

Yang, F., & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. *ASIA & THE PACIFIC POLICY STUDIES*, 5(3, SI), 533–543. doi:10.1002/app5.246