RIGHT TO INFORMATION: BALANCE BETWEEN STATE SECURITY AND RIGHT TO PRIVACY

AUTHOR

Dr. ASM Mahmudul Hasan

DUJAR

RIGHT TO INFORMATION: BALANCE BETWEEN STATE SECURITY AND RIGHT TO PRIVACY

AUTHOR

Dr. ASM Mahmudul Hasan[1]

EDITOR

Professor Dr. Ali Asker[2]

[1] ORCID: 0000-0001-8833-5101

[2] ORCID: 0000-0003-1801-3371

Right to Information:
Balance Between State Security and Right to Privacy
AUTHOR: Dr. ASM Mahmudul Hasan

Editor in chief: Berkan Balpetek
Editor: Prof. Dr. Ali Asker
Cover and Page Design: Duvar Design
Printing : March -2026
Publisher Certificate No: 49837
E-ISBN: 978-625-8572-85-8

853 Sokak No:13 P.10 Kemeraltı-Konak/İzmir
Tel: 0 232 484 88 68
www.duvaryayinlari.com
duvarkitabevi@gmail.com

Library Record Card
Right to Information: Balance Between State Security and Right to Privacy
Hasan, ASM Mahmudul 173 pages, Bibliography included.

TABLE OF CONTENTS

Abstract

In a democracy, a fundamental part of the citizen's right to information (RTI) is to provide a means for citizens to participate in the system of government, and to hold their governments accountable to them through transparency. However, the implementation of the RTI has frequently encountered resistance based on competing claims for national security and the protection of private citizens' personal and private information. The absence of legal standards regulating the resolution of conflicts arising from these two competing interests has led to protracted, ongoing tensions between the two throughout most of the world, typically resulting in excessive privacy, weakened accountability and oversight, and diminished confidence in the government. This study examines how RTIs can be used effectively in the context of the competing claims of national security and the right to privacy of citizens. The study uses a combination of doctrinal and analytical legal research methodologies, as well as comparative methods of analysis. The study analyzes a variety of documents, including international human rights conventions, soft law, judicial precedent and domestic laws. The study examines the relationship between RTI and freedom of expression and democratic theory, the legal basis for privacy and national security, and how conflicts between the two are handled. The study includes a focused case study of Bangladesh's RTI enacted in 2009, which assesses the law against both international standards and domestic realities. The study demonstrates that RTI, privacy and national security are not inherently incompatible with one another. The primary source of the conflict is the imprecision of existing definitions, overly broad exemptions and the lack of effective oversight mechanisms in the law. The study also demonstrates that the use of necessity, proportionality, harm-based assessments and override to public interest are vital to formulating an effective balance between the competing principles. Finally, the study indicates that the use of RTI is undermined by the inability to create a coherent legal relationship between RTI and older secrecy laws; thus, transparency is significantly undermined by

these older laws. This study creates new knowledge (i.e., analytical framework that treats RTI, privacy and security interdependently in a single unified model) and offers an analytical framework to align the principles of transparency, privacy and security so that they can be reformed as a whole. This study provides suggestions for legal reforms that improve accountability and transparency in a manner that balances the legitimate claims of privacy and national security.

Keywords: Right to Information, State Security, Right to Privacy, Transparency and Accountability, Democratic Governance

List of Abbreviations

ACHPR – African Charter on Human and Peoples' Rights

CEDAW – Convention on the Elimination of All Forms of Discrimination against Women

CRC – Convention on the Rights of the Child

ECtHR – European Court of Human Rights

FOI – Freedom of Information

FOIA – Freedom of Information Act

HRC – Human Rights Committee

ICCPR – International Covenant on Civil and Political Rights

ICESCR – International Covenant on Economic, Social and Cultural Rights

NGO – Non-Governmental Organization

OSA – Official Secrets Act

RTI – Right to Information

RTIA – Right to Information Act

UDHR – Universal Declaration of Human Rights

UN – United Nations

Preface

In contemporary democratic governance, access to information held by public authorities has emerged as a central legal and normative concern. The Right to Information (RTI) is increasingly recognized not merely as an administrative entitlement, but as a foundational mechanism through which transparency, accountability, and public participation are realized. In an era marked by expanding state functions, complex security challenges, and unprecedented data collection, the demand for openness has intensified alongside concerns relating to state security and the right to privacy. These developments have rendered the relationship among transparency, secrecy, and personal autonomy one of the most contested issues in modern public law.

The evolving relationship between RTI as an individual legal entitlement and the protection of personal privacy is grounded in the political principles of free speech and the right to democratically self-govern. At present, the RTI has evolved into a legally autonomous right protected under international human rights law and constitutional law and has been incorporated into domestic law in many countries around the world. The increasing enactment of RTI laws worldwide indicates a consensus exists that the foundation for democratic legitimacy is the availability of general citizenry that is informed and institutions that are accountable to citizens. Consequently, one of the practical and legal challenges that has arisen from the enactment of RTI legislation is when government must balance the need to disclose information against national security claims, or when government must balance personal privacy with the obligation to disclose information under RTI laws.

The position of state security is of extreme sensitivity within the legal framework in which it exists. Often, governments cite national interest, order and the collective safety of people as

justification for maintaining secrecy surrounding security matters. Although the concerns to justify maintaining secrecy are often reasonable, there is vast evidence to support that when security claims are vague or needless expansive, they provide an excuse for excessive secrecy, abuse of power and evading accountability. Likewise, the right to privacy, which is stated to protect citizen dignity and autonomy, is frequently improperly applied to restrict access to public interest information that contains public officials or public resources.

These considerations raise a number of important legal questions. How should the legal system balance the right to know with the competing rights to privacy and security? Where do the limits of secrecy belong in a democratic nation? What standards belong to the legal system to maintain limitations on transparency as being exceptional, justified and proportional?

This book will address these questions through a legal analysis and a comparison of various legal systems to examine the relationship between both the right to know and the right to privacy with state security. It posits that the interests outlined above are not mutually exclusive but must be balanced fairly through a principled legal analysis. The study satisfies that transparency and secrecy are complementary elements of governance in a democratic society and each has valid but limited purposes.

At an international level, this book investigates the theoretical underpinnings of the right to access information from a human rights law perspective, and how it can be understood in relation to the values associated with freedom of expression, as well as its applicability to economic, social and cultural rights. The book particularly examines developing standards that set out the circumstances when it is possible for the access to information to be lawfully restricted, with the Tshwane Principles on the Right

to Information and National Security being a primary resource for assessing current balancing approaches.

At a national level, this book provides a more detailed examination of Bangladesh; the Right to Information Act, 2009 signified a marked improvement in the establishment of transparency within the state. The Act is aligned with international standards both regarding its objectives and structure, however, its implementation continues to demonstrate legislative, institutional and cultural difficulties. The unique and persistent conflicts that exist with older secrecy laws; administrative opposition; limited capacity to exercise oversight over the implementation of the Act; and a significant lack of societal awareness continue to impede the implementation of RTI. By situating Bangladesh within a larger comparative framework, this book highlights shared difficulties between other developing democracies and significant jurisdictional barriers that prohibit the growth of democratic governance within Bangladesh.

In terms of methodology, the study adopts a doctrinal legal methods approach, supplemented by analytical and comparative methodologies. Primary legal sources, international instruments, judicial decisions, and academic scholarships have been used to compile the study. The study is constructed in accordance with a continuum, moving from the analysis of conceptual foundations to normative framework considerations, and finally, practical application and reform-based assessment.

Finally, the core conclusion of the book is that the extent to which the right to access information is effective is less about its legal recognition as a right, as much as it is dependent upon the extent to which balance mechanisms exist and are used effectively. In order for transparency to be protected from excessive secrecy and for legitimate privacy and security interests not to be diminished, clear definitions of laws; narrowly

defined exemptions; independent oversight; proportionality analysis; and public interest principles must exist. Through an application of a coherent analytical framework, and its application on both international norms and the Bangladeshi experience, the study aims to enhance understanding of how democratic legal systems may govern the flow of information, while doing so in a manner that is transparent, accountable and rights-respecting. This book draws upon research originally undertaken in the author's Master's thesis, defended in 2014.

CHAPTER ONE

FOUNDATIONS, PROBLEM STATEMENT, AND NORMATIVE FRAMEWORKS

SECTION 1: INTRODUCTION

1.1 Background of the Study

The right to information (RTI) is one of the most important developments in governance and law of the late 20th to early 21st century. RTI establishes that all democratic and developing countries have a legitimate right of access to the information held by public entities like government Departments. Governments have now agreed that RTI is a key tool for creating transparency, promoting accountability and allowing for participatory governance. The increasing emphasis placed on RTI over the past several decades is indicative of a much broader change in the relationship between governments and citizens, where secrecy is no longer assumed to be the default position of government; rather, secrecy will generally require a legal justification (Relly & Sabharwal, 2009; Roberts, 2005).

The empirical and legal research evidence suggests that access to information held by government is fundamental to improving the quality of governance. Increased transparency will promote well-informed public participation in the governmental process, enhance the ability of governmental institutions to be accountable, and strengthen the ability of citizens to monitor and review all decisions that fall under the authority of government (Bauhr & Grimes, 2012). Thus, RTI is not just an administrative convenience, but an integral element of democratic legitimacy. Citizens simply cannot assess how effective or efficacious a government service or policy is when they do not have access to the necessary information required to evaluate it, challenge it, or hold the government accountable for any possible abuses or acts of corruption or incompetence (Bertot et al., 2009).

When looking over the last 20 years of RTI legislation across the world and its increase in acceptance as a right, one can see a clear trend. The vast majority (80+) of countries have created and adopted Right to Information or Freedom of Information laws by the early 2010's. These laws are created by both developed and developing countries, which indicates that all forms of government are beginning to align their democratic, international human rights agenda with the reform of their governance model that is being encouraged by some international organizations and activist organizations (Roberts, 2010). With this, there has come recognition that there is a close connection between RTI and other large development goals, such as good governance reforms, anti-corruption initiatives, and the rule of law.

While countries have created RTI legislation, the implementation of RTI laws has resulted in continuous tensions among what the law aims for. The idea that transparency is a virtue of a democratic society has been balanced against other interests that a country has a legitimate interest in asserting and therefore restricting access to information. For example, countries tend to always include state or national security and individual privacy in addition to other permissible withholding reasons. It is the balancing of competing legal and normative interests in the area of RTI that has produced "new" discussions on access versus balance between transparency, state/national security, and individual privacy.

1.2 Evolution of the Right to Information as a Human Right

The right to access information is a human right, and it has grown from the evolution of the principle of freedom of expression under international law. Initially, access to information was considered a sub-component of the freedom of expression associated with the freedom of press. Access to information was not considered a separate legal right until early

in the 20th century. The formal recognition of the right to information began in 1948 with the adoption of Article 19 of the Universal Declaration of Human Rights (UDHR), which provides for the right "to seek, receive and impart information and ideas through any media and regardless of frontiers" (United Nations, 1948). Article 19 of the International Covenant on Civil and Political Rights (ICCPR), which was adopted later, strengthened the legal basis of Article 19 of the UDHR by creating an obligation on state parties to comply with the ICCPR. As Article 19 was interpreted, the early focus of the interpretations was on the right to impart information. However, over time, judicial and academic interpretations began to place greater emphasis on the right to seek and receive information with respect to public authority (McDonagh, 2013). The heightened focus on the right to seek and receive information is a significant step toward recognizing RTI as an independent human right, separate from freedom of expression.

By the early part of the 21st century, several constitutional courts and human rights bodies had recognized RTI as a constitutional or quasi-constitutional right. Peled and Rabin (2011) support this assertion by noting that there is a growing consensus that a democratic form of government requires both the existence of a right to freedom of expression and that there be affirmative obligations on the state to provide information. This development reflects the evolution of RTI from a negative right (freedom from interference) to a positive right (an entitlement to institutional mechanisms, procedures and remedies).

The presence of international and regional human rights organizations also supported this development. According to the Human Rights Committee, interpretations made by treaty bodies initially recognized access to information about public authorities as necessary for fully enjoying civil and political rights. As a result, RTI has become accepted as a basic

component of democratic participation, accountability, and other human rights (McDonagh, 2013).

1.3 Conceptual Tension Between Transparency and Secrecy

The right to know is increasingly being recognized, but it faces continuous challenges because of the historical focus on keeping information private by governments. Secrecy has often been used to maintain control; protect sensitive information; and reduce political risk for governments. In many ways, the resistance to openness and transparency by public agencies (Roberts, 2005) is demonstrated through the use of administrative delays, a variety of exemptions, and use of discretion in how to apply laws requiring agencies to provide information to the public.

Since the events of September 11th, and during and following the end of the Cold War, the combination of increased fears associated with terrorism; the expansion of collections of intelligence; and the heightened focus on national security has put increased pressures on governments and other public agencies, resulting in an increase in the number of laws, regulations, and policies designed to prohibit the release of information to the public. Caidi and Ross (2005) observed that the relative lack of restraint imposed on the actions of governments has resulted in many countries enacting overly restrictive policies regarding the release of information to the public. This "securitization" of government policy towards information is reflected in the increasing number of requests for government information being denied because they are classified as confidential rather than being granted by an agency.

It is also important to note that this distinction - between transparency and secrecy - does not have a neutral status. Although transparency is often associated with democratic accountability and secrecy with executive efficacy and security,

a binary construct is not an accurate boundary condition. While there are legitimate public benefits associated with absolute transparency, some functions of government may be negatively impacted by absolute transparency. Conversely, excessive secrecy may have a negative effect on public confidence in and legitimacy of governments.

For these reasons, many authors maintain that the definition of secrecy must be limited and that secrecy must be viewed as the exception rather than the rule (Roberts, 2005; Bauhr & Grimes, 2012). Without proper limits on the use of secrecy and proper oversight of the use of secrecy, secrecy may be used as a means of avoiding accountability; concealing wrongdoing; or stifling public debate. This paradox forms a key element of many contemporary discussions of RTI and also informs the conflict between privacy and national security.

1.4 State Security and Privacy as Competing Legal Interests

State security and the right to privacy are two of the most complicated legal interests that have been outlined as limited by the right to know (RTI). Both state security and the right to privacy are legitimate public interest grounds for denying individuals access to information; however, both also can be applied inappropriately and/or over extended. The interplay among state security, right to privacy, and RTI gives rise to a number of fundamental questions, such as proportionality, necessity, and democratic oversight.

While there is no universally accepted definition of state/national security within International Law, it is generally defined to include the protection of the territorial integrity, constitutional order, and populations of the state from serious threats. The state commonly uses the national security argument to deny access to information related to national defense, intelligence or foreign relations. Researchers have conducted

empirical studies, which indicate that the security argument is used invalidly to apply a broader interpretation of “sensitive” than is warranted, including information that is used to limit access to information referring to routine administrative functions (Caidi & Ross, 2005).

Similarly, privacy is a form of protection against state intrusion into an individual's life and acts as a counterbalance to transparency by allowing for an individual's right to privacy. Privacy promotes the dignity, dignity, and personal integrity of an individual, and is recognized as a fundamental right to all people under international human rights law. A conflict arises when there is an attempt to get access to personal data in the context of their requesting information from an individual, such as an employer, obtaining their health records, or law enforcement. Privacy limitations in the RTI context can be the most common argument used to deny access to information; however, there is often a lack of clarity around the privacy limitations that exist (Turle, 2007).

The main challenge is how to balance state/national security and the right to privacy against the public's right to have access to public information. Banisar (2011) provides a further note of emphasis about the nature of those competing interests and the identification of those interests being placed as “over” or “under” the public's right to know. Security and privacy should not be absolute barriers to granting access to RTI; rather, their application must be limited by, grounded in law, and subject to a public interest test. There should be a presumption of access to information in regard to public interest matters such as corruption, human rights violations or abuses of power, even when there may be legitimate national security/privacy concerns associated with that information.

The complex relationship between RTI, state security, and privacy provides a basis for the principal inquiry of this

dissertation. Therefore, it is essential to develop a coherent legal framework for access to information that results in respect of an individual's rights by better understanding how RTI, state security, and privacy laws intersect, are in conflict with one another and can be reconciled through the application of legal principles of access to information.

1.5 Statement of the Research Problem

Although RTI has been widely accepted as a cornerstone of democratic governance, its practical enactment has not yet reached the same level of acceptance. Many jurisdictions have legislated RTI (and freedom of information) laws; however, many of those same jurisdictions have effectively undermined their implementation through overly broad exemptions, resistance from administrators and expansive interpretations of competing interests (especially state security and the right to privacy). Secrecy continues to remain, as an administrative culture, the default in many jurisdictions, inhibiting the potential for change created by RTI (Roberts, 2005; Bauhr & Grimes, 2012).

One of the main problems in relation to the ability to invoke national or state security to deny access to information is that those terms are often deceptively ambiguous and overbroad. The fact that most legal systems have not established precise legal definitions and have not created effective oversight mechanisms has allowed those systems' authorities to withhold information that is neither a real risk to national, state or individual security, nor is it identifiable as such (Caidi & Ross, 2005). The practice of using national or state security as grounds for nondisclosure diminishes accountability as required under RTI and reduces public confidence in governmental authorities. Likewise, while protection of privacy rights are also necessary for protecting the dignity and autonomy of individuals, privacy is often used in a way that favors the use of confidentiality over transparency without appropriately assessing the public interest (Turle, 2007; Banisar, 2011).

Another factor creating tension between these interests is the absence of coherent frameworks to provide for the balancing of RTI against privacy or national security in an even-handed consistent fashion. Many legal systems provide no tests based on legality, necessity or proportionality to provide a principled basis for making decisions; consequently, decision-making is often ad hoc or results in inconsistent outcomes. Therefore, RTI is at risk of being little more than a formalized right without real-world effect and, as a result, will be incapable of supporting accountability or democratic engagement in the way that was intended (Peled & Rabin, 2011).This book will seek to address this deficiency by considering how best to balance RTI against national security and privacy in both international human rights law as well as national legal systems, with a specific focus on contexts in developing countries.

1.6 Research Questions

This research will use the following questions to examine how the Right to Information (RTI) has developed as a human right within international law:

(1) What is the historical evolution of the right to information as a human right and its various legal frameworks?

(2) What are the main legal arguments for restricting access to information under RTI on the grounds of national security and protecting the right to privacy?

(3) How do existing RTI legal regimes exist in balancing transparency with legitimate concerns of national security and the right to privacy?

(4) How have international law or standards and academics interpreted or provided guidance on the principles to be used when addressing conflicts between the right to information, the right to privacy, and the need for national security?

(5) What lessons can be learned from comparing the practices of different countries that can help improve the coherence and efficacy of RTI systems, especially in developing countries?

The purpose of these questions is to define the normative basis for RTI, identify infrastructure weaknesses in current methods for balancing interests in favor of media disclosure, and assess the adequacy of existing legal protections.

1.7 Objectives of the Study

This research project intends to thoroughly analyze the legal framework governing the RTI and its connections to state security and the right to privacy. More specifically, this research project has six specific aims; to: (a) investigate the international legal standards that establish that RTI is a human right; (b) evaluate the definitions and limitations of state security and privacy as lawful restrictions on RTI; (c) look at the relative balance of competing RTI standards; (d) find evidence of abuse or excessive application of security and privacy limitations thereby obstructing RTI; (e) develop principled criteria for competition between RTI and other interests which reflect democratic principles and human rights; and (f) advance the scholarly and policy dialogues surrounding RTI by developing and offering a cohesive framework suitable to both developed and developing countries.

By fulfilling these goals, this study will increase the theoretical consistency of RTI and improve its utility as a means of promoting accountability and good governance (McDonagh, 2013, Banisar, 2011).

1.8 Research Methodology

The legal research methodology is based on doctrinal methodologies and complemented by analytical and comparative methodologies to understand the legal relationship between the right to information (RTI), right to privacy, and rights to national security.

The methodological approach of this book uses doctrinal legal research as a base methodology. This means systematically studying legal authorities, such as international treaties, constitutions, statutory laws, case law, and other authoritative interpretations of international and domestic treaties made by a treaty body or court. The goal of this research is to ascertain the legal rules, principles, and standards governing the right to have access to information and what legal limitations apply to that right (Hutchinson & Duncan, 2012).

Using the doctrinal analysis approach, this research examines how RTI is defined by international human rights law, how restrictions due to security and privacy are justified according to that law, and whether those restrictions meet the required legal tests of legality, necessity, and proportionality. This methodology is particularly well suited to evaluating the degree to which there is normative coherence and doctrinal consistency across a variety of legal systems.

The analytical and comparative aspects of this research methodology provide additional value. The analytical aspect focuses on the reasoning behind the rules of law and how they affect transparency and accountability. The comparative aspect analyzes how selected national and international jurisdictions have balanced RTI with competing interests through comparison. The goal of using comparative analysis as this research's analytical and comparative component is not to determine the best or worst legal system; instead, the goal is to extract generalizable principles that could provide effective RTI frameworks particularly in developing countries. The combination of these three methodologies provides a fuller view of the normative ideals and the operative issues associated with the RTI legal regime.

SECTION 2: CONCEPTUAL AND THEORETICAL FRAMEWORK OF THE RIGHT TO INFORMATION

2.1 Meaning and Definition of the Right to Information

The RTI frequently switched with Freedom of Information (FOI) in addition to the Right to Know - can be perceived as a legal right which allows individuals to obtain information held by public authorities except where it is legally exempt. The RTI is not simply an administrative ideal for promoting openness; it is a rights claim against the State based upon democratic principles and international human rights standards and is enforced through institutional action which creates entitlements (Mendel 2003, McDonagh 2013).

A complete definition of the RTI comprises four inter-related components or elements:

1. Right Holder (who can possess the right): The General principle is that everyone/citizens according to different legal systems would be the right holders for RTI, with contemporary RTI frameworks describing access rights broadly under the premise that all records maintained by a public authority (The state) are held by officials for the benefit of the public (Ackerman & Sandoval-Ballesteros 2006, Mendel 2003).

2. Duty Holder (who must provide the information): Since RTI creates positive obligations upon public authorities to provide the requested information, it will also require these agencies to publish selected categories of information. This marked a significant transition from the classical notions of "negative liberties" to a new model where the State assumes responsibility for the use of procedures, the maintenance of records, and the responsiveness of institutions (Mendel 2003, Peled and Rabin 2011).

3. Object of the Right (the meaning of the word "information"): RTI entitles citizens to access all recorded (documented) public information, regardless of whether it is held in traditional formats such as paper documents, electronic files, e-mail or other formats. It includes the right to access both raw material and materials produced as an outcome of the Government's policies. In essence, after the above three elements taken together, the right to access is established, the concept is that citizens can access all types of records in some manner through a public authority, either through creation or acquisition by the public authority (Mendel 2003).

4. Procedural Enforceability: RTI becomes effective and practical only when implemented by established procedural protections: specifiable time limits, reasonable fees, legally defined exemption criteria/requirements, the obligation to provide reasons for refusals and an independent oversight mechanism (Mendel 2003; Roberts, 2005).

The comparative perspective on RTI also includes how structural principles define the “models” of openness that have been created within these systems. The following four principles maintain broad-based acceptance among early RTI scholars as foundational components of the overall theory as espoused in the literature:

- Maximum disclosure / presumption of openness (i.e., there is a presumption that everything will be disclosed; anything said in secret must have a justification),

- Limitation on the exceptions (i.e., exemptions should be defined narrowly and when necessary),

- Independent oversight (i.e., there should be administrative or judicial review), and

- Promotion of open government (i.e., proactively publish information and maintain records for the purpose of promoting open government) (ARTICLE 19, 1999; Mendel, 2003).

A critical theoretical point regarding RTI is that it focuses on more than the right to access information; it is also concerned with creating an equalized informational relationship between those who govern and the governed. It disputes the existence of secrecy as a prevalent administrative culture, while simultaneously positioning public information as a precondition for citizenship, participation, and accountability (Roberts, 2005; Peled & Rabin, 2011). Thus, RTI has come to be recognized as a constitutional value (or even constitutional right within some countries' jurisdictions) that provides citizens with not only an instrument for efficient governmental operations but also an attribute of pure democratic legitimacy (Peled & Rabin, 2011).

2.2 RTI, Freedom of Expression, and Democratic Theory

In its role as the basis for creating an international standard of law to recognize the human right of RTI, the most important characteristic of the RTI Declaration is that the right to access information is a component of freedom of expression, particularly to seek and receive information. While the protection of freedom of expression is often framed as a way to protect speech, it is based on something deeper—meaningful expression cannot exist without the existence of information that permits the individual and community to develop opinions, evaluate government performance, and engage in a common life (McDonagh, 2013).

From a legal standpoint, RTI can be viewed as fulfilling three democratic functions:

(a) The informed citizen function: In order for citizens to evaluate their government's performance, there must be

access to information regarding the government's policies, expenditures, and management of its resources, or else citizens cannot make informed decisions when voting or engaging in the public debate about government issues. RTI reduces the differences in information between the public and state institutions, allowing citizens to scrutinize the reasoning, decisions and results of governmental actions. (Roberts, 2005; Relly & Sabharwal, 2009).

(b) The deliberative public sphere function: The quality of public reasoning is essential to the legitimacy of a democracy. In this respect, the "public sphere" is not merely a meeting place for different opinions but is also the point of exchange of reasoning between citizens and institutions, and for the exercise of power. RTI enhances the public sphere by creating access to the rationales behind government policies, records of regulations, and records of administrative procedures, which would otherwise be secret (McDonagh, 2013; Peled & Rabin, 2011).

(c) The accountability function: The fundamental protection of free expression provides individuals with a basis to criticize the government based on the existence of documentary evidence. Investigative journalism, civil society monitoring, and parliamentary oversight rely on access to documents. Censorship and the obstruction of access to documents (whether through 'spin control' or administrative obstruction) have the same effect on democracy as any other form of censorship—while censoring speech, they also prevent the individual from having access to the information necessary to make a reasonable critique of the government (Roberts, 2005).

The significance of the relationship between RTI and freedom of expression is heightened in the context of contemporary information systems. As democracy continues to rely more upon digital spaces as the means for democratic communication, access to and circulation of information becomes necessary for a democratic culture. With this in mind, Balkin's work with regard to digital speech and democratic culture illustrates this point, namely that there are two components to a democratic freedom of expression in an information society: (1) the absence of censorship; and (2) structural conditions that provide opportunities for people to participate in, access, and have communicative power in relation to the digital space (Balkin, 2004). Accordingly, RTI is linked to contemporary democratic theory not only as a legal right but as a structural condition necessary for democracy to function effectively.

The relationship between RTI and freedom of expression does not suggest that RTI exists in an absolute form. Rather, democratic theory recognizes that there may be circumstances in which the government can legitimately refuse to disclose specific information, such as where disclosing that information would endanger national security or would infringe on an individual's right to privacy. However, as a theoretical matter, the burden is on the government to justify and explain why it is withholding information and the restrictive conditions must not be the norm within that culture (ARTICLE 19, 1999; Roberts, 2005).

2.3 RTI as a Precondition for Good Governance

"Good Governance" generally refers to good governance principles and conditions. These include (but are not limited to) the following: Transparency; accountability and answerability; responsive to public needs; opportunities for participation; and rule-based governance. RTI (Right to Information) plays an important role in the four aspects defined above because, at their roots, failures in governance begin as failures of information

because of the lack of access to key decisions, lack of access to records of how decisions have been made, lack of access to how funds were spent and other similar forms of secrecy (Bertot et al., 2009; Bauhr & Grimes, 2012).There is evidence to support the hypobook that there is a direct positive relationship between good governance and the perception of governments and governance being better due to transparency. A cross-national study (Relly & Sabharwal, 2009) found that there is a direct relationship between how the people perceive the policymaking of the government and how credible public institutions are. It also reinforced the idea that governments being open to the public is a legal goal and that while it is not the same thing as the quality of an organization or its institutions, it can have a direct impact on the amount of confidence the public has in its government, which can be seen as an important resource for good governance.

In using an institutional theory perspective, RTI promotes good governance through at least four mechanisms:

1) Reduction of information asymmetries. Generally, policy information is available to the public through the policy authority. RTI decreases information asymmetries by making it more difficult to provide unjust or illegal policy and processes (Roberts, 2005; Mendel, 2003);

2) Increase in administrative accountability. If an official knows his/her record may be made publicly accessible to other public officials, he/she may change the way he/she keeps accurate records and make decisions. While this will not eliminate abuse of the administrative system, it will increase the "cost" of arbitrary decisions by an official's actions (Roberts, 2010; Bertot et al., 2009);

3) Strengthening the oversight ecosystem. By providing documentary access to the records of public officials, RTI strengthens the ecosystem of oversight by creating more accountable journalists, civil society groups, auditors and

parliaments. This is significant in providing oversight systems in contexts that have little or no traditional checks and balances (Roberts, 2010; Grimes, 2008);

4) Supporting e-governance and public service delivery. Most information provided by government has been generated and is stored in an electronic (digital) format in modern governments. Bertot, et al. (2009) demonstrate how government information policies intersect with e-government and the public's right to access it. These examples show how RTI continues to be important as a form of government reform in how governments manage information and to whom that information will be made available.

Although there are significant reasons to believe that there is a positive relationship between RTI and good governance, RTI is not automatically equal to good governance. Bauhr and Grimes highlight that there are significant differences in defining, measuring and assessing degrees of transparency. They state that transparency is a condition of organizations that has an impact on whether or not the government is functioning in the capacity as a good or successful organization and there is an important research related point in that RTI will promote good governance if and only if the law is implemented and has oversight and remedies.

2.4 Transparency, Accountability, and Anti-Corruption Frameworks

The common view is that RTI is often defended as a transparency tool; however, transparency is valuable primarily due to its connection to accountability. Conceptually, accountability includes at least two elements:

- answerability (the obligation to explain and justify decisions) and

- enforceability (the ability to take disciplinary action or enforce corrective measures in the event of a breach of duty). While RTI provides information to support answerability, there must be additional institutional mechanisms (i.e. oversight entities, courts, auditing systems, and political repercussions) in place for effective enforcement of accountability. Thus, transparency cannot be used as a substitute for accountability.

Fox argues persuasively that unless transparency can be connected with mechanisms to make use of the information to impose consequences, the relationship between transparency and accountability is ambiguous. Fox highlights that "transparency" can be weak or strong: weak transparency may present an illusion of being open and subject to oversight, but strong transparency will provide actionable information that will enable effective accountability processes (Fox, 2007). This distinction is especially important in RTI regimes where information is technically accessible but practically obstructed by delay, cost, or overly broad exemptions.

Lindstedt and Naurin make a closely related argument; transparency alone typically does not reduce corruption unless there are institutional systems in place to act on disclosed information. Their comparative study indicates that the effectiveness of transparency in reducing corruption will depend on whether or not citizens, the media, and oversight entities can interpret information and mobilize appropriate accountability responses (Lindstedt & Naurin, 2010). In the case of RTI, this suggests that disclosure protocols should be combined with strong institutional competencies, both within government itself (i.e., record-keeping, compliance) and within society (i.e., independent media and civil society monitoring).

RTI is an effective anti-corruption method, but only because it helps reveal the types of information that can allow corruption

to stay hidden. Corruption relies on secrecy, especially the secrecy of procurement, licensing, public appointments, and budget execution. Making access to records available through RTI makes it more likely that wrongful behavior is uncovered and contested (Roberts, 2010). For example, Roberts' analysis of the RTI in India has been cited frequently to show how it can serve as a valuable tool in the struggle for accountability, as civil society entities can often make strategic use of disclosure rights (Roberts, 2010).There is an essential role for civil society in this regard. Grimes' case study survey data indicates that civil society engagement can be critical for combating corruption, but success typically depends on a number of factors, such as political opportunity, institutional responsiveness, and the availability of usable information (Grimes, 2008). This means that RTI is not acting alone in the fight against corruption; it is acting within a broader system of accountability.

In conceptual terms, this results in a book-relevant framework:

- RTI → Transparency (disclosure of information)
- Transparency + Oversight Capacity → Answerability (justification, scrutiny)
- Answerability + Enforcement – Institution → Accountability (consequences and rectification)
- Accountability → Impact on Corruption Prevention (deterrent effect, exposing activity, reforming activities).

This framework illustrates why RTI laws can exist in "theory", while corruption is still occurring; unless there are enforceable levels of accountability combined with credible oversight, transparency will likely be a formality. Similarly, when RTI is supported by independent oversight and responsive institutions, it increases the likelihood that those involved in corrupt activity will be detected (Fox, 2007; Lindstedt & Naurin, 2010; Roberts, 2010).

2.5 RTI as the “Mother of Rights”

The Right to Information's naming as "mother" indicates a substantial claim. The right to access information is not just one of many rights, but an enabling, foundational right that is necessary for the fulfilment of the enjoyment of other civil, political, economic, social and cultural rights. Academically, judicially, and in international advocacy, this argument has become more apparent with respect to democratic governance and the accountability of human rights.

The underpinning premise of the argument is that rights have no meaning to a person unless the person has access to the information that a person needs to be able to understand, assert the right, and enforce the right. In the absence of information concerning laws, policies, administrative actions and available remedies, rights are abstract and inaccessible. Birkinshaw (2006) has argued that freedom of information acts as a structural right which provides the foundation for openness, legality, and accountability in public administration, and therefore facilitates the realization of other substantive rights (p. 179-183).

This establishing function is demonstrated throughout the different right categories. In relation to civil and political rights, the ability of citizens to access information enables the citizen to monitor the electoral process, monitor law enforcement activity, and challenge the exercise of power. In relation to economic and social rights, access to information relating to budgets, delivery of services, eligibility for services, and the priorities of government policies will prove crucial to assessing whether government obligations are being fulfilled. In this respect, RTI is perceived as a gateway right which has the ability to change the legal entitlement framework into a mechanism for the citizen to assert a claim (Mendel, 2003).

The "mother of rights" also connects to the theory of democracy. In Sen's compelling discussion of democracy's

intrinsic, instrumental, and constructive value, he argues for an important theoretical foundation. Sen's argument regarding the instrumental value of democracy, as an instrument against abuse and to meet the needs of society, rests substantially on the principles of openness and public access to information (Sen, 1999, p.10-12). RTI creates the instrumental support for democracy by allowing informed participation and public reasoning.

The constitutional framework for RTI is provided in the works of Peled and Rabin (2011) who address the fact that some jurisdictions have constitutively recognized RTI as a functional right because of its systemic significance. Their research demonstrates increasing recognition by courts that there is a direct link between access to information and the ability of the people to exercise popular sovereignty and engage in self-governance through democracy. This constitutional recognition reinforces that RTI is required in order to sustain the normative framework of everyone's rights.

Although viewing RTI as "the mother of rights" does not imply absolute rights exist, it emphasizes the functional priority of RTI. If limitations are placed on access to information, then justifications for such limitations will only survive with a higher standard of justification — as limiting access to information will limit the effective enjoyment of multiple other rights. This understanding will be especially significant in future discussions regarding proportionality, public interest override and balancing frameworks.

2.6 Limits of the Right to Information

RTI is a fundamental principle of access to information, but it has never been the absolute right. RTI legislation and international law accept that, in some cases, there can be reasons for restricting access to information. The challenge is not determining whether there are restrictions, but how those restrictions will be defined, justified and enforced.

Going from a human rights perspective, restrictions on RTI should follow the basis of what would generally apply for a restriction on fundamental human rights. Therefore, they should be based on legality, legitimate aim, necessity, and proportionality. While these criteria have most clearly been stated in respect of the protection of freedom of expression, they have also been applied consistently when it is under an RTI analysis (McDonagh, 2013, pp. 34-38).

Mendel's research of legislation around the world has found legitimate reasons for the restriction of access to information are typically found in areas of national defense, international relations, law enforcement, privacy rights, commercial confidentiality and the protection of deliberative processes. He does caution, however, that they must be interpreted narrowly and not impose a blanket exclusion (Mendel, 2003, pp. 21-24). If a broad exclusion is applied to RTIs, this can turn RTI from a right into a discretionary privilege.

Legal theory supports this caution. In terms of the principle of proportionality, scholarship in public law has established that any restriction will limit an individual's right to the least extent necessary in order to achieve the legitimate purpose of the restriction. Prof Craig's discussion of proportionality assures that any measure limiting a right will only achieve its aims and will only have a connection to the aims of the legislation (Craig, 2011, pp. 268-272). Thus, this means that for RTI, justification for secrecy must not be supported through abstract or speculative risk, but on an identified and concrete harm.

In literature there has been an ongoing and commonality related to a cultural acceptance of hiding things. According to Roberts (2006), governments often use secrecy as a way to avoid embarrassment and hold themselves politically accountable, instead of to protect legitimate interests. Therefore, this creates an imbalance between access to information and restrictions and reduces the normative effect of RTI legislation.

Therefore, RTI restrictions must be applied as an exception and should only be enforced based on strict construction, reason giving, and independent review. Using this theoretical structure will allow public interest doctrine and function as a way to address issues of overbroad secrecy.

2.7 Public Interest Doctrine in RTI Laws

The public interest doctrine is an integral aspect of RTI systems overall. The public interest doctrine establishes that an exemption may still allow the disclosure of information if it is within the public's best interest to do so. Essentially, this redefines RTI as doing away with rigid rule-based systems and instead being evaluated according to context-sensitive factors.

As far as theory is concerned, the public interest doctrine demonstrates a progression from categorical secrecy to reasoned justification. According to Calland (2010), the public interest doctrine helps create democratic accountability by requiring decision-makers to provide clear justification of how information may be beneficial to society when making decisions about what documents are released; thus, eliminating the reliance upon formal classification alone to make these decisions (pp. 4-6). This practice adheres to the principles of democracy that prioritize transparency when it enhances citizens' ability to participate, oversee government, and protect their own rights.

Studies offer evidence that the public interest overrides are extremely important in relation to information about acts of corruption, misuse of government resources, violations of human rights, and threats to public health or safety. In these situations, there is often a high societal value in releasing this information. In the absence of meaningful public interest tests, privacy or security exemptions can easily be abused as a way for a government agency to avoid being accountable by obscuring wrongdoing, and many scholars believe that this undermines the ability of RTI to operate effectively to provide information to the public (pp. 10-12).The

public interest doctrine mediates between RTI and different competing rights by establishing that both privacy and security are legitimate interests, but that these interests are sometimes subordinate to the larger societal interests. This is consistent with the philosophical tenets of democracy, in that rights are interrelated and should not be viewed as separate from each other.

Roberts (2006) indicates that without a meaningful public interest override for requests specifically related to information in this digital age, RTI systems have the potential to become very complicated and difficult to obtain substantial information, as there will continue to be extensive use of exemptions for the sole purposes of not releasing records, even though they may be accessible from a technical standpoint, as well as through careful and conservative interpretations by the agencies responsible for reviewing them.

For this reason, the public interest doctrine serves a normative role by guaranteeing that RTI is able to achieve its underlying purpose of a democratic society and not merely become an exercise in rigid compliance.

2.8 International Normative Foundations

International normative developments provide the basis for both the conceptual and theoretical framework around the right to information (RTI). Early international instruments regarding human rights do not explicitly mention "the right to information"; however, they established the basis for its recognition by providing for the right to seek and receive information as part of the overall human right of the freedom to express oneself. The textual bases of this development can be found in Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR).

Over the years, national institutions of interpretation increasingly indicated that, to effectively exercise their freedom of expression, individuals require access to information maintained by public

authorities. McDonagh (2013) details this evolution, illustrating how international institutions moved from the negative conception of non-interference to a more positive understanding of state obligations to facilitate access to information (pp. 27-33). Additionally, soft-law instruments and expert principles provide further normative guidance on RTI. The Article 19 Principles on Freedom of Information Legislation outlined normative standards for RTI, including maximum disclosure, restrictive exclusions, and independent oversight, which were used as a practice reference point for domestic RTI legislation globally (ARTICLE 19, 1999). While not legally enforceable, these principles have had considerable normative weight.

Meanwhile, scholarly interpretations of Article 19 of the ICCPR reinforced the belief that access to information is also fundamental for democratic participation and accountability. According to Nowak, restrictions on access must be read narrowly, and they must be justified on a strict basis of necessity and proportionality (Nowak, 2005, pp. 442-447). In addition, Joseph, Schultz, and Castan emphasize that access to information enables citizens to monitor government actions and to pursue redress for violations of their rights (Joseph et al., 2004, pp. 399-402).

As a result, access to information has developed as a recognized norm within the broader discourse of international human rights. Although it has not yet been uniformly codified as a separate stand-alone right, it is internationally accepted as a prerequisite for democratic governance and protection of human rights, and thus the normative underpinnings upon which the subsequent balancing of competing interests-primarily privacy and state security-will occur will be grounded.

SECTION 3: RIGHT TO INFORMATION UNDER INTERNATIONAL LAW

3.1 RTI in International Human Rights Law

International law approaches the right to information as an interpretive development in the context of human rights, instead of as a single globally codified "right to information treaty", with the strongest legal basis for the right to information being based upon (i) freedom of expression norms, in particular the "seek and receive" dimension, (ii) the right to participate in public life and (iii) a growing obligation to adhere to institutional transparency as a part of accountability in democratic governance (United Nations, 1948; United Nations, 1966; Human Rights Committee, 2011).

A well-known foundational international recognition of the normative significance of access to information is contained in UN General Assembly Resolution 59(I) of 1946, which states that the freedom of information is a fundamental human right and a "touchstone" for the freedoms enshrined within the UN (United Nations General Assembly, 1946). While the Resolution was adopted before the establishment of modern treaty systems, it is doctrinally relevant because it articulates "freedom of information" as a structural condition necessary for establishing peace, and progress, and human dignity. As the Resolution indicates, it is not surprising that later developments in international human rights law increasingly recognize access to information as more than just a bureaucratic preference; rather, it is increasingly being recognized as a right.

In terms of its doctrinal analysis, the right to information encompasses both negative and positive aspects. The negative aspect protects individuals, as well as the media, from censorship and from improper (i.e., without justification) governmental interference in the flow of information. The positive aspect relates to a government's obligation to facilitate access, for

example, by maintaining records, implementing processes for providing access to information, and providing remedies when access to information is denied. Mendel's comparative and international analysis demonstrates that many of today's right to information laws were developed in recognition of the fact that the right to access to information held by the government can only meaningfully be realized if there is a procedural architecture—for example, time limits on access, reasoned refusals of access, narrow exemptions to access, and the provision of independent review for refusals of access (Mendel, n.d.). While procedural elements are, for the most part, treated as administrative, in terms of human rights, the procedural elements are implements through which the government meets its obligation to uphold human rights.

The relationship between accountability and democracy has been defined by international law relating to Human Rights and also due to RTI, as it allows citizens access to documents that may violate human rights through transparency and can hold governments accountable (Subrahmanyam, 2002, pp.258-263). The argument surrounding access to information by those who control information would also be consistent with the concept of human rights, in concerns of where the government or state holds critical pieces of information (such as legislation, government expenditure, detention, or regulations), and by blocking access, would impact the practical rights citizens have and potentially affect oversight.

There has also been some agreement within the International community on the premise that there is some level of recognition that access to information held by a Public Authority exists as a form of free expression and would therefore be a protected right. This is evidenced through the Human Rights Committee's General Comment No. 34 (2011) on Article 19 ICCPR which identified access to information held by Public Bodies as a form of free expression and that access cannot be denied unless there

are strict standards of legality and necessity (Human Rights Committee, 2011). General Comments are not a legal instrument, but rather an authoritative interpretation and can therefore support doctrine.

To summarize, RTI under International Human Rights sector is not a stand-alone doctrine, it is a cross section of multiple areas of law such as Freedom of Expression, Democratization, Good Governance and Accountability. The cross-section of such laws supports the book of the work. Because RTI is based on the principle of Fundamental Rights, any limitation based on State & National Security or Privacy should be evaluated as a limitation on Rights and as such, can only be restricted where the Restriction can be justified.

3.2 Article 19 of the UDHR and ICCPR

The current normative foundation of RTI first came about with Article 19 of the Universal Declaration of Human Rights (UDHR) in 1948 and its corresponding treaty - Article 19 of the International Covenant on Civil and Political Rights (ICCPR) in 1966 - which both state, amongst other things, that everyone shall have the right to search for, receive and communicate information and ideas without interference. This phrasing supports more than expression; it grants all individuals an entitlement to access information that is necessary to create their views or take part in being a part of public life (United Nations, 1948; United Nations, 1966). Although the UDHR is a declaration and not a treaty, it provides two normative functions that support the notion of RTI: it develops the substantive grammar of rights; and it creates the base level for the formation of other treaties. Article 19 contains the expansive right to access information as a part of the right to freedom of expression, as it articulates the active right to search for information and the passive right to obtain such information.

By making article 19 of the ICCPR binding and creating treaty provisions, the ICCPR implements the principle of article 19 in the UDHR into the existing body of treaty law. ICCPR, article 19(2), carries forward the reference to searching for and receiving information and makes it apparent that access to information through all means and across all borders is guaranteed - therefore guaranteeing that access to information is not limited to just through the traditional press (United Nations, 1966). Article 19(3) also creates the canon of restrictions on the right to access information: all restrictions must be established by law and necessary to achieve a legitimate (i.e., protect the rights/reputation of another, protect national security, protect public order, protect public health or morals) aim; meaning that any access restriction based on security or other similar grounds would need to meet high levels of justification as they involve access to a protected freedom (Subrahmanyam, 2002, pp. 258-263). General Comment No. 34 provided clarity to the Human Rights Committee on how Articles 19 of the ICCPR and the UDHR relate to RTI and access to information. The Committee explained that article 19 of the ICCPR provides for a right of access to information held by public bodies, and that countries should take positive steps to provide for RTI through proactive disclosure, and should establish procedures that provide such access; contact between RTI and state security and/or privacy restrictiveness must also meet strict necessity requirements and proportionality requirements (Human Rights Committee, 2011). Additionally, this interpretation is also significant from a scholarly point of view, as it demonstrates the legal connection between expression and access to public information for purposes of establishing criteria for assessing when access to government information should be restricted; thus, meeting the basic tenets of RTI.

The following are the three implications of Article 19 as it relates to the relationship between RTI, state security and state privacy:

1. RTI is tied to a right under the seek and receive portrayal of expression; therefore, the denial of access to RTI is a right's related issue (United Nations, 1966; Human Rights Committee, 2011).

2. Restrictions are legally constructed and not discretionary; that is, they must be provided through law, for a legitimate purpose, are necessary and proportional to the legitimate goal (United Nations, 1966).

3. The state bears the burden of demonstrating that the state security or state privacy justification for restricting access to RTI is valid because the restrictions are exceptions to the protected freedom. This is consistent with the doctrine of transparency as a right enunciated throughout the literature (Subrahmanyam, 2002, pp. 258-263).

Therefore, articles 19 of the UDHR and ICCPR serve as not only an ethical basis for RTI, but also provide a doctrinal framework for assessing and determining whether state secrecy is either lawful or a violation of state obligations to protect human rights.

3.3 Jurisprudence of the Human Rights Committee

The Human Rights Committee (HRC) has greatly contributed to the transformation of the theoretical guarantee of the right to freedom of expression in Section 19 of the ICCPR into a reality-based enforceable right to receive information. The ICCPR does not expressively state there is an implied "right to receive information," but the HRC's legal reasoning considered with its interpretation and application of authority (including General Comments and individual communications) has gradually clarified that the right to receive information (typically held by a Public Authority) is an inherent part of the freedom to seek information and the right to receive information.

Initially, the HRC was primarily concerned with negative limitations on freedom of expression, such as restrictions on speech by communicating this with a Representative of a Public Authority. As the HRC developed its Interpretation, the HRC recognized that if a person does not have access to necessary information that would allow them to form an opinion and participate in the public affairs processes, then their freedom of expression is meaningless. This change in understanding represents a broader trend towards recognition of human rights and an evolution away from a solely non-interference model toward an understanding of a solely positive obligation model.

The HRC's legal reasoning was most recently articulated in General Comment No. 34 (2011). In this comment the HRC makes it clear that the scope of Article 19 includes an implied right to receive information held by public bodies and any limit on access to information held by public bodies must comply with the limitation requirements under Article 19(3) of the ICCPR. The HRC states that the States shall have affirmative procedural obligations (e.g. freedom of information legislation) to enable Implementation of this implied right to receive information (Human Rights Committee, 2011, paragraphs 18-19) and is of considerable importance to an RTI book completed in 2013 due to having defining laws regarding RTI's implied under the ICCPR up to that point in time.

While the HRC has not produced a sufficient body of cases to support an explicit determination on the Right to Receive Information cases, the HRC's legal reasoning in the cases on Procedural Transparency, Access to Records, and State Accountability strongly aligns with the Right to Access Information. Analysis of HRC legal reasoning by the Redress Trust indicates that the HRC has consistently stated that access to relevant information is a necessary component (but not sufficient) to enable exercise of rights, including the Right to Effective Remedy in Article 2(3) of the ICCPR (Redress Trust,

2006, pages 155-160). In other words, when a state prevents or refuses to provide access to information that would allow a person to claim a violation of their rights (tortures, arbitrary detention, or forced disappearance) the state is committing an act incompatible with its obligations under the ICCPR.

This line of reasoning provides an essential basis for linking RTI with both Article 19 and provides both procedural justice and a remedy when there is a denial of access to information. Access to Information is therefore a necessary means of enforcing multiple rights and reinforces the book argument that RTI is an enabling right within the International Human Rights System.

The HRC establishes two significant principles regarding the balancing of RTI, State Security and Rights to Privacy:

1. Presumption of Access: All information held by Public Authorities are subject to Article 19 and the burden is on the State to justify the denial of access as a limitation of a protected right (Human Rights Committee, 2011).

2. Strict Scrutiny of Restrictions: Justification for Denial of Access based on National Security, Public Order, and the Rights of Others must meet the standards of necessity and proportionality. An abstract or speculative harm does not satisfy either standard.

Consequently, the HRC provides a Rights-Based Framework to evaluate Secrecy. The HRC establishes that International Law does not treat Access to Information as a matter of pure administrative discretion, and therefore, is a matter of legally enforceable Human Rights.

3.4 RTI in Economic, Social, and Cultural Rights

Access to information is a key enabler for achieving the rights that define economic, social and cultural rights (ESCRs) across multiple dimensions. There is no explicit right to access

information in the International Covenant on Economic, Social and Cultural Rights (ICESCR), but the Committee on Economic, Social and Cultural Rights (CESCR) has repeatedly stated that the accessibility of information is vital to many rights recognized in the Covenant. The CESCR consistently interprets the Covenant to require "... the availability, accessibility, acceptability [and] adaptability" of all ESCRs (General Comments apply) based on widespread consensus by 2013.

Right to Health

Right to health under Article 12 of the ICESCR includes access to information as one of its core components. In General Comment No. 14, (2000), the CESCR emphasizes that ‘accessibilities’, as one of the fundamental features of the right to health, extend to the right to seek, receive and impart information on health matters, except in cases of confidentiality regarding personal health data (CESCR, 2000, para. 12(b)).

London's examination of a human rights-based approach to health points out that accountability in health systems requires transparency and access to information to enable the public to hold the appropriate authorities accountable for policy decisions, resource allocation and service availability (London, 2008, pp. 69–72). As such, individuals and communities must have access to information in order to assess states compliance with the obligations imposed upon them or to challenge the state in relation to discriminatory and arbitrary practices. This makes it possible for individuals and communities to use their right to information to participate in the realization of their right to health, as well as monitor and claim their right to health, and reinforces RTI as an enabling right among the ESCRs.

Right to Food

Right to adequate food under Article 11 of the ICESCR is also dependent upon access to information. In General Comment No.

12 (1999), the CESCR states that all States Parties must adopt transparent strategies and account for their efforts with respect to food security and the various measures they employ to combat food insecurity; therefore, access to information must be provided as per the requirement of General Comment No. 12 (1999) (CESCR, 1999, para. 23).

Narula provides a thorough examination of the right to food and outlines how access to information, including access to the details of a States agricultural policy, as well as the mechanisms of food-aid administration, is important for holding both States and international actors accountable (Narula, 2006, pp. 700–710). Furthermore, affected populations are able to determine whether policies that are in place will contribute to the advancement of food security or merely reinforce inequality when they have access to information regarding budgets, subsidies, and distribution frameworks. In summary, the right to information is an essential precondition to the enjoyment of, and its enforcement, as a right to food, particularly in contexts of poverty and structural vulnerability.

Right to water

The CESCR's General Comment No. 15 (2002) defines the relationship between RTI and ESCRs as noted above with respect to water. The Committee states that all individuals and groups should have full and equal access to information about water issues, including information about water services, and the environmental conditions in which such services are provided (CESCR, 2002, paras. 48–49).

Bluemel provides an example of this type of analysis where he concludes that transparent information is instrumental in assessing water allocation decisions, water quality, and water pricing (Bluemel, 2004, pp. 980–985). Therefore, affected communities are unable to participate fully in decision-making processes or challenge harmful practices without access to such

information. Thus, RTI is not an ancillary right, but rather, intrinsic to the substance of the right to water.

Right to Education

The right to education recognized in Articles 13 and 14 ICESCR incorporates access to information in its various aspects as related to availability, accessibility, acceptability and adaptability. In General Comment No. 13 (1999), the CESCR establishes that States Parties are required to establish a transparent and effective system for monitoring compliance with their educational obligations and the educational standards in the Covenant (CESCR, 1999, paras. 49, 54).

Tomasevski provides similar comments and concludes that RTI regarding curricula, funding, admission standards, and quality standards is necessary for parents, students and the wider Community to determine whether their education system meets its obligations under the Covenant (Tomasevski, 2001, pp. 23–27). In general, RTI provides the means to exercise oversight over education, participation in education decisions, and obtain redress from violations of their rights.

Across all four ESCR areas, a consistent theme arises: access to information is a necessary condition for exercising substantive rights. International human rights law acknowledges RTI as an element of civil and political rights as well as a structural element of justice and accountability in society. This observation supports the greater point of the book: when State Parties restrict access to information related to health, food, water or education under the grounds of privacy or national security, such restrictions must be analyzed under both Article 19 ICCPR and under the obligations imposed by the ICESCR; and excessive secrecy around these issues has the potential to create obstacles to the realization of fundamental social rights.

3.5 RTI in Women's Rights (CEDAW)

According to the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), there is a clear link between the right to information (RTI) and women's rights. While CEDAW does not directly assert that there is a right to know in general, repeatedly it embeds access to information as an essential precondition for women's effective enjoyment of their rights, especially in education, health, family life, and public participation.

CEDAW is based on the principle of substantive equality that mandates not only formal legal guarantees but also removing structural barriers, which prevent women from exercise their rights. The lack of access to information, as to laws, services, reproductive health or government policies has been identified as one of those barriers for a long time. Cook states that the asymmetry of access to information affects women more than anyone else, with the greatest impact in contexts with social inequalities and gendered power structures (Cook, 1994, pp. 510-515).

Article 10(h) of CEDAW obligates State Parties to provide women access to educational information regarding family health and family planning. Implicit in the language of this provision is the recognition that access to information is a prerequisite for independent decision making and autonomy. In the absence of access to accurate and timely information, legal guarantees of equality are rendered ineffective.

CEDAW link access to information and women's right to health by requiring states under Article 12 to eliminate discrimination in access to health services, including reproductive health. Current scholarship has shown that in order for women to control their bodies and make health related choices, women need access to information regarding services, risks and rights related to health (Byrnes, 2010, pp. 430-

434).From a human rights perspective, the denial of information is considered both an administrative failure and gender-based discrimination, particularly where secrecy/lack of transparency negatively impact women to a greater degree.

RTI also promotes women's engagement in public life and political action. Access to information regarding public decision making, budgets, and policy priorities permits women's organizations to engage in advocacy and oversight. The CEDAW Committee has consistently stated in its concluding observations that in order for women to effectively participate in and monitor a States compliance with its obligations under CEDAW and broader international standards, states must provide both transparency and access to information.

Doctrinally, RTI within the CEDAW framework is an enabling right that supports:

- Informed decision making
- Substantive equality
- Accountability to gender sensitive policies.

As a result, any restrictions invoked by the state based on privacy, morality, or security that restrict access to information about women's rights must be analyzed very carefully to avoid reinforcing discrimination or undermining the object and purpose of CEDAW.

3.6 RTI in Child Rights (CRC)

The Convention on the Rights of the Child (CRC) provides one of the clearest treaty-based recognitions of the right to access information as at least part of the treaty itself, in addition to other instruments dealing with human rights; the CRC's clear statement that children have the right to seek, receive and impart

information provides a very direct normative basis for the right to access that information under child rights law.

Under Article 13(1) of the CRC, children are guaranteed the right to freedom of expression which includes freedom to seek, receive, and impart information and ideas of all kinds through any media of their choice. The provisions of Article 13(1) parallel those of Article 19 of the International Covenant on Civil and Political Rights (ICCPR), except that the provisions of Article 13(1) are tailored specifically to the status and needs of children as rights-holders rather than as passive recipients of protection (Detrick, 1999).The CRC's provisions regarding access to information are related to the principle of evolving capacities which requires respect for children's autonomy and participation progressively with their development. Lansdown (2005, pp. 305-309) has demonstrated that appropriate access to information is generally critical to children having enough access to participate in informed decision-making regarding education, health care, and family life.

From this perspective, the right to access information is more than just an abstract right to access state-held information; it also requires that children's access to that information be appropriate, comprehensive, and understandable based on their level of development and capacity.

The access to information is also a way to protect child rights. The provision of information regarding how to access legal remedies, child protection services, and information regarding the procedures of social service and legal systems can be used as a way for children and their representatives to challenge outcomes resulting from abuse, neglect, and exploitation. The CRC Committee has previously stressed that a lack of transparency in institutions that provide services to children (e.g., schools, detention facilities, and group care) increases the likelihood of child rights violations.

Moreover, access to information held by public authorities, e.g., records relating to child welfare, education standards, and the juvenile justice system—is essential for monitoring the compliance of the state with their obligations under the CRC. In this way, access to information reinforces accountability mechanisms within the overall child rights governance system.

The access to information is a child right that, like many other human rights, is not without limits. Article 13(2) of the CRC allows for limitations on the right to access information in the context of protecting the rights of others, national security, and ensuring public order. Still, the international child rights framework consistently requires that limitations on the right to access information be interpreted narrowly and in a manner consistent with the best interests of the child principle. Overbroad reliance on national security and parental authority as justification for restricting children's access to information is likely to undermine children's autonomy and participation.

Under the framework of the CRC, the right to access information has two functions:

- It empowers children as holders of rights; and
- It enhances transparency and accountability of institutions who provide for children's welfare.

As a result of the two functions of the right to access information, the book makes a broader argument that restrictions on access to information are cross-cutting rights and that such restrictions require careful justification.

3.7 RTI in Democratic Governance Instruments

While core human rights treaties do reference the right to information (RTI), an explicit reference to RTI as a concept and practice is highly associated with democratic governance by the ways in which instruments used for implementing democratic

governance turn abstract rights into standards of public administration. In particular, two areas of instruments have emerged that were especially significant in establishing this relationship, Commonwealth principles and the Johannesburg Principles on National Security, Freedom of Expression, and Access to Information. These instruments represent the collective consensus of the Commonwealth countries and commonwealth states on best practice and also serve as interpretative tools for applying binding human rights norms, though neither represents a conclusion.

Commonwealth countries and states support access to information as a prerequisite for citizens to democratically participate in and hold their governments accountable; they have formalized that public participation in the governance of a country is only meaningful when there is sufficient access to official information. The Commonwealth Law Ministers' Meeting Communique (1980 and reaffirmed in 1999) further supports this interpretation by stating that there is a clear link between access to official information and democratic participation in governance (Roberts, 2005, pp. 2-6). While various Commonwealth initiatives established concepts related to RTI, those implemented through either model legislation or technical guidance generally support the idea of: i) proactive disclosure; ii) limited exemptions from disclosure; and iii) independent oversight of RTI processes.

These same initiatives support the notion that secrecy is the exception to the rule and should be justified, and they are consistent with restrictions set forth in Article 19 of the ICCPR concerning the use of restrictions on the human right to access information (Article 19 ICCPR).The Johannesburg Principles represents a critical milestone in the attempt to balance RTI and national security. Developed by experts in their respective fields of law, the principles have been widely accepted and cited by courts and UN bodies (Johannesburg Principles, 1995).

The principles explain that access to information may only be restricted where the disclosure will create an imminent threat to the existence or territorial integrity of a state and are not based solely on the potential embarrassment or wrongdoing of the government. Academia has pointed out that such a limitation is included in the principles to combat misuse of security concerns by the government to impede accountability (Caidi and Ross, 2005, pp. 670-674). With regard to human rights violations, the Johannesburg Principles emphasize that information concerning human rights violations may never be legitimately withheld on national security grounds. This further strengthens the case that RTI is critical for accountability in relation to transitional justice and that governments may not use secrecy as a tool to block redress.

Together, Commonwealth principles and the Johannesburg Principles operationalize RTI within democratic governance by:

- clarifying the scope of permissible secrecy,
- reinforcing the presumption of disclosure, and
- providing interpretive guidance for balancing RTI against security claims.

They therefore serve as an essential bridge between treaty law and domestic RTI regimes, particularly in developing democracies.

3.8 State Obligations and Permissible Restrictions

As noted above, international law recognizes that there are neither absolute rights with respect to access to information nor is there an unqualified obligation for states to provide access to information. Instead, international law creates a systematic structure of obligations for states to respect, protect and fulfil access to information, while providing for restrictions only under clearly stipulated circumstances. Such a systematic structure of

provision and limitation on the access to information had developed as a result of the provisions contained in International Treaties, General Comments and Principles of Governance.

The positive obligations of states to provide access to information include:1. Establishing a legal framework to enable access to information held by public bodies (such as RTI laws);2. Providing procedural guarantees, including clear request processes, time limits, the right to request reasons for denial and the ability to independently appeal (Mendel, n.d.); and3. Engaging in the proactive disclosure of public information, particularly where access to information is essential in order to participate in decision-making or hold officials accountable for their actions (Human Rights Committee, 2011, para. 19).The positive obligations of the state reflect the recognition that without institutional capacity and procedural clarity, the right to access to information cannot be effectively enforced.

The restrictions that may be imposed on the right to access to information must meet the three-part test under Article 19(3) of the ICCPR:

- Legitimacy - the restriction must be provided by law that is adequately accessible and easily understood;
- Legitimate purpose - such as national security, public order, or the protection of others' rights; and
- Necessity And Proportionality - the restriction must be the least restrictive alternative available to achieve the legitimate purpose and must be proportionate to the purpose being achieved (UN, 1966; Human Rights Committee, 2011).

Many scholars have suggested that the burden falls on the state to demonstrate the justification for any restrictions on access to information, and that the state must provide concrete

and specific justifications rather than relying on abstract claims (Banisar, 2011, pp. 10-14).

Among the most commonly cited justifications for restricting access to information are national security and privacy. However, international standards are clear that:

- Security arguments must be specific and demonstrate a real risk of harm (Johannesburg Principles, 1995);
- Privacy exemptions must apply only to information that is genuinely personal and NOT to hide offences of public significance, such as corruption or abuse of power (Szekely, 2009, pp. 296-301).

Whenever possible, partial access to the requested information and/or the redaction of the requested information is more appropriate than a blanket denial of access, and this has been recognized as a good practice in access to information regimes (Banisar, 2011).The systematic structuring of the provision of and conditions for restricting the right to access to information is central to the main inquiry of this book. International law does not purport to deny the validity of secrecy, but seeks to constrain the concept of secrecy through the application of rights-based tests. Therefore, the interested parties of State Security and Privacy are not absolute; instead, they are two competing and qualified interests that must be balanced against the democracy-enhancing and rights-promoting function of access to information.

SECTION 4: RIGHT TO PRIVACY—LEGAL FOUNDATIONS AND SCOPE

4.1 Concept and Meaning of Privacy

Privacy has been a contentious and central concept in legal thought since its inception. While many definitions exist, privacy can be best described as a constellation of divergent interests which curtail access to people, information, and decisions that are integral to maintaining individual autonomy and dignity. The classic scholar of privacy, Ruth Gavison argues that multiple dimensions of the human experience resist reduction to a singular formula, and thus, privacy cannot be circumscribed, but rather will include multiple experiences and means (Gavison, 1980, pp. 423–425).

Ruth Gavison is often quoted for her analytical framework for approaching privacy, which she defines as limited access to individuals. Under Gavison's approach, privacy consists of achieving a relative condition of physical, informational, and decisional inaccessibility to others (Gavison, 1980, pp. 428–433). In a legal context, one of the significant implications of this restricted access to an individual is that it helps to delineate privacy from secrecy; privacy can have the same degree of protection as an acceptable restriction on the access of others.

Another perspective is Joseph Thomson's theory of privacy, in which privacy is understood to encompass a derivative right over an individual's body, property, and information that collectively protect personal autonomy (Thomson, 1975, pp. 300–304). Within this theoretical framework, privacy violations result from others infringing upon those rights without an individual's consent or lawful justification. As such, privacy claims can be found arising in many different contexts, such as: monitoring of individuals, data processing, bodily integrity, and family life, for example.

Subsequent developments in theoretical thought have further refined the concept of privacy by focusing on context. In her theory of contextual integrity, Helen Nissenbaum argues that privacy is protected when information flows through social networks in accordance with pre-existing norms and standards associated with social roles, social interactions, and normative standards associated with the transmission of information (Nissenbaum, 2004, pp. 122–127). From this understanding, privacy is only violated when information has been shared inappropriately — beyond social norms, thus subverting the social meaning of the various roles contained within the social network. This observation is critical to the new reality of digital governance and data-rich administration, where individuals will be sharing information multiple times a day, often without an understanding of their social context.

Julie E. Cohen's analysis of informational privacy deepens our understanding of privacy from a conceptual standpoint through her exploration of the nexus between privacy and self-development. Cohen contends that the increasing prevalence of surveillance and data aggregation, transforms individuals into objects of constant surveillance by serving as impediments to their ability to develop freely as a citizen within a democracy and as a person (Cohen, 2000, pp. 1377–1383). Hence, Cohen notes that privacy can no longer be understood as an individual's preference, but rather must be viewed as a structural condition necessary for autonomy within contemporary societies.

Taking all of these perspectives together, privacy includes: (1) Spatial and bodily privacy (freedom from physical intrusion); (2) Informational privacy (ability to control your personal information and records); and (3) Decisional privacy (the ability to make choices pertaining to the individual in an autonomous manner without interference).Thus, for the purposes of this research paper, I will conceptualize privacy to be the fundamental legal interest serving to protect an individual's

dignity and autonomy through restricting unauthorized access to the individual and to personal information. This conceptualization is crucial when considering the extent to which privacy will constitute a legitimate basis for limiting the right to information (RTI) and/or when privacy claims may be inappropriately used to shield state conduct from public scrutiny.

4.2 Historical Development of the Right to Privacy

The concept of the right to privacy wasn't created all at once; it has evolved through a combination of common law, constitutional law and international human rights norms. The development of the legal history of privacy as a concept primarily arises from the famous article entitled, "The Right to Privacy," written by Samuel D. Warren and Louis D. Brandeis in 1890. This article was written as a response to the intrusive nature of journalism at the time and advances in photo technology. The authors established privacy conceptually to be the right of an individual to be left alone, which they argued is the foundation of personality and human dignity (Warren & Brandeis, 1890, pp. 193-195). Although privacy was ground in the law of tort at the time, Warren and Brandeis created a framework that would drastically shape future constitutional and human rights decisions regarding privacy.

Judges and scholars in the 20th century sought to further categorize and systematize the various privacy claims. One of the most well-known and influential classifications of privacy created by William Prosser identifies four categories or torts of privacy: intrusion upon seclusion, publication of private facts, false light, and appropriation (Prosser, 1960, pp. 389-392). Prosser's categorization of privacy torts provided various judicial tools that have shaped judicial decision making regarding privacy throughout much of the United States.

As we moved through the 20th century, privacy was afforded a constitutional basis in a growing number of jurisdictions.

Constitutional analysis by Jed Rubenfeld demonstrates that constitutional privacy protects much more than simply secrecy, but serves to create two major protections: (1) protecting one's most fundamental choices and (2) limiting arbitrary state power (Rubenfeld, 1989, pp. 740-746). In addition, international privacy scholarship demonstrates that while many Anglo-American legal systems and societies have historically grounded privacy in concepts of liberty and freedom from interference, many European legal systems and societies have historically grounded privacy in concepts of dignity and personality rights (Whitman, 2004, pp. 1153-1160).

In the late 20th century, there again was an increase in concerns for privacy due to advances in technologies related to surveillance, computing and data processing. Gormley provides an excellent historical chronicle of the manner in which each major technology introduced from the invention of photography to the arrival of databases prompted a fundamental rethinking of how to protect privacy rights (Gormley, 1992, pp. 1338-1345). This period of privacy in the late 20th century helped to provide the conception of modern day data protection and the recognition of informational privacy as a legal right.

In addition to these domestic developments related to privacy, international recognition of privacy also occurred through international instruments, culminating with the adoption of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. The concept of privacy had been firmly established as a universal human right applicable to state surveillance, capture of data and administrative decision making. The historical evolution of privacy is important because it shows that privacy as a concept is fluid and ephemeral. It has evolved as societal needs and state power have evolved. Furthermore, the evolution of privacy has been characterized by the need to achieve a proper balance between protecting the privacy of individuals versus providing the public good. An

understanding of this historical evolution is necessary to understand the modern conflict between privacy, the right to information and state security – the primary focus of this book.

4.3 Privacy, Human Dignity, and Autonomy

Privacy is a fundamental human right associated with human dignity and autonomy. Privacy is much more than a way of keeping your personal information secret; in fact, it is a way of developing your personality, making moral choices, and participating in social and political life.

Human dignity is one of the main underpinnings for modern constitutions and international laws against human rights. Dignity implies that all individuals are to be treated as ends in themselves, and not just objects of state control. Privacy protects that status by providing individuals with the ability to limit invasive observation, surveillance, and disclosure that could cause them to be treated as mere information sources. According to Gavison (1980), once a person is fully available to others (especially states), that person cannot create their own identity and their own relationships (pp. 441-445).The European conception regarding the relation between privacy and dignity is clearer than in the United States. Based on Whitman's (2004) comparative study, in continental Europe privacy represents an individual's honor, personality and social standing; it is not meant to be simply a liberty interest (pp. 1161-1166). Because of this, many jurisdictions consider the violation of an individual's privacy as a great affront to that individual's worth as a human being, regardless of whether there is tangible harm.

Privacy is also a source of personal autonomy. Autonomy is understood to be the capacity to make meaningful choices about your life without being coerced or manipulated. Given this context, Thomson (1975) demonstrates that violations of privacy function to decrease an individual's autonomy by reducing that individual's ability to control his or her body, personal

information, and intimate choices when someone violates that individual's privacy (pp. 305-309).

Cohen (2000) also discusses how privacy can be viewed in relation to the conditions that are required for self-development in a democratic society. Monitoring (surveillance) and data profiling inhibit individuals' ability to experiment, dissent, and create independent judgments; therefore, privacy is a necessary condition for creating democratic citizenship (pp. 1404-1410). Thus, privacy is not an obstacle to transparency, but rather that privacy is necessary for an individual to be able to participate meaningfully in their community.

The connection between privacy and asymmetries in power, from individuals to the government, should be emphasized based upon the dignity-autonomy framework. Through "surveillance," data retention, and unregulated information sharing, governments have developed a significant amount of power over individuals, often without their knowledge or consent. Privacy serves as a countervailing force against arbitrary power and creates an environment for individuals to be independent of each other (Rubenfeld, 1989, pp. 784-789).This insight may demonstrate the core of this book: while having transparency and access to information is required for the accountability of a democratic society, unregulated access to personal data, regardless of whether it is justified through national security or administrative efficiency, may ultimately destroy the dignity and autonomy that human rights principles aim to protect.

4.4 Privacy in International Human Rights Law

The acknowledgement of privacy as a basic human right marks an important turning point in the legal history of privacy. International human rights law sees privacy as more than just a domestic concern, but has also seen privacy as an internationally recognized obligation on States when dealing with surveillance, data collection and the disclosure of information.

For example, Article 12 of the Universal Declaration of Human Rights (1948) states: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.

Although the UDHR does not have the force of law, it has been instrumental in creating treaty law and establishing constitutional practices. In addition, Article 12 has established two key elements:

(1) privacy is a broad category; it covers family, home, correspondence and reputation, and

(2) interference must not be arbitrary. In this way, legality and reasonableness were incorporated early on as a requirement for interference with an individual's privacy.

There is also academic commentary that the prohibition against arbitrariness was intended to create the basis for later-developed doctrines of necessity and proportionality, which are ultimately the tools used to balance the individual's right to privacy against competing interests such as national security and public order (McDonagh, 2013, pp. 31-33).

The International Covenant on Civil and Political Rights (ICCPR, 1966) transforms the UDHR's normative commitment into binding law. Article 17 provides:

1. "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence…"

2. "Everyone has the right to the protection of the law against such interference or attacks."

Article 17 introduces two cumulative standards: interference must be neither unlawful nor arbitrary. The Human Rights Committee (HRC) has clarified that even lawful interference may

be arbitrary if it is unreasonable, disproportionate, or unnecessary in the circumstances (Human Rights Committee, General Comment No. 16, 1988, para. 4).

Under Article 17, states bear both negative and positive obligations. Negatively, they must refrain from unjustified intrusions into private life. Positively, they must adopt legislative and institutional measures to protect individuals from privacy violations by public authorities and, increasingly, by private actors (HRC, General Comment No. 16, para. 1).

This dual obligation is particularly relevant for RTI regimes. While states are required to disclose information in the public interest, they must simultaneously ensure that disclosure does not result in unjustified exposure of personal data, especially where such exposure serves no legitimate public purpose.

International human rights law thus does not treat privacy as an absolute barrier to transparency, nor as a residual interest easily overridden by security claims. Instead, it establishes privacy as a normatively robust right that can be limited only under strict conditions. These conditions—legality, necessity, proportionality, and protection against arbitrariness—form the legal framework within which conflicts between RTI, privacy, and state security must be resolved.

4.5 Constitutional Protection of Privacy

Privacy is now considered more important than it was before, because constitutional protections have been placed into the legal order of a nation. Some constitutional protections do not directly mention privacy in them, but they protect it indirectly by other rights like liberty, dignity, and freedom of expression. Since World War II, many new constitutions have referenced and protected both privacy and additional concepts such as the inviolability of homes or confidentiality of communications. For example, many European constitutions have recognized privacy

as part of personality rights, which have a close relation to human dignity (Whitman, 2004).

On the other hand, the American Constitution does not expressly contain a right to privacy. The right has come about through constitutional interpretation of privacy interests derived from guarantees of liberty and due process. According to Rubenfeld, judicial reasoning has used privacy as a limitation to the power of government and not only as being able to keep private things confidential (Rubenfeld, 1989).

Comparative constitutional law scholars have found a significant difference regarding how privacy rights are protected in dignity or liberty-based systems. In dignity-based systems, generally located in Europe, the right to privacy is a form of protection of the moral and social identity of an individual, and an infringement of this right will be treated as an infringement of personhood. In liberty-based systems, privacy is a protection of freedom from the government (Whitman, 2004).

Despite this conceptual difference, the courts throughout jurisdictions have relied upon common standards for the analysis of privacy interferences, such as legality, necessity and proportionality in their assessments. These standards allow for the privacy restriction to be justified by compelling public interests and being affected narrowly.

Finally, Constitutional protections of privacy are particularly important if a country has a right to information (RTI) law. If privacy is in the Constitution, then RTI laws must be construed in a manner consistent with constitutional privacy guarantees. This means that the obligations placed on governments to be transparent are not to supersede or defeat the obligation to protect privacy automatically, but rather, an appropriate constitutional balancing test must be done to protect privacy. The balancing test will require particular careful attention to situations where the government is disclosing personal information regarding citizens

who have given their citizens personal information to the government.

4.6 Informational Privacy and Data Protection

One of the greatest advancements in today's privacy law is the development of the newest form of privacy known as informational privacy. Informational privacy deals with how personal information is gathered, processed, housed and shared by state actors and big institutions.

While early forms of privacy protection were based upon notions of secrecy from physical invasions of privacy, enormous advances in technology and computer systems have created new forms of risk to privacy through large scale monitoring and profiling. Cohen argues that during this period understanding informational privacy as secrecy alone is insufficient rather, it must be understood in context of an individual's right to be free from systematic surveillance and manipulation of behavior that is based upon the individual's personal records (Cohen, 2000).With this shift came the introduction of data protection frameworks that allow for the processing of personal information as opposed to prohibiting the processing of personal information. Data protection frameworks recognize the importance of the flow of personal information to support good governance; however, they also require safeguards against the misuse of personal information.

Data protection frameworks are based on several core components:

- Lawfulness and fairness of processing personal information
- Specified objectives for which information can be processed
- Minimizing the amount of personal information collected

- Ensuring the accuracy and security of personal information
- Providing individuals with access to their personal information for purposes of correction and, in some cases, for deletion.

Bygrave argues that these components are established to help restore balance in the power between data controllers - typically the state - and individuals to allow individuals the ability to maintain autonomy in an overly information (or data) reliant society (Bygrave, 2010).

European data protection law has heavily influenced the establishment of global standards regarding informational privacy and data protection. Schwartz states that the European approach to establishing data protection laws encompasses a focus on the dignity of the individual and controlling their personal information. In addition, European laws include restrictions on the transfer of personal information outside of the European Union to jurisdictions where individuals do not receive adequate protection (Schwartz, 1995). The concepts established in European data protection laws have been influential throughout the past decade in the development of privacy protection laws, particularly in the area of developing legal norms, and establishing respect and dignity of the individual in legal debate, and informing privacy protection based on the principles that should be followed in developing privacy protections (including, information protection). The principles established by the European regime continue to influence the development of data protection laws and privacy protections in developing countries (by including the principles) globally.

The nature of the interaction between data protection laws and RTI is multifaceted as noted by Banisar as while RTI promotes transparency, data protection laws routinely add privacy-based exceptions to the disclosure of personal information. When the

data protection framework is properly designed, the frameworks are not oppositional; they complement each other: the framework of RTI provides information that exposes the abuse of power, and the framework of data protection protects individuals from becoming collateral damage due to the exercises of transparency.

For the purposes of this book, informational privacy, and data protection provide the legal framework through which the conflict between RTI and privacy can be solved, by and through the operationalization of constitutional and human rights concepts through the translation of abstract values (i.e. dignity, autonomy, and proportionality) into enforceable normative requirements.

4.7 Legitimate Limitations on Privacy

Despite the fact that it is considered to be a fundamental human right, privacy is still subject to limitations. Domestic and international laws accept that limitations may legitimately be imposed on privacy if they pass certain stringent legal tests. The legitimacy of these limitations helps us understand how privacy interacts with competing interests such as transparency, public order and national security.

The primary requirement for any limitation on privacy is that it be provided for in law. This rule protects individuals from arbitrary interference by ensuring that laws with respect to the interference with privacy are accessible, clear, and do not give public authorities unfettered discretion to interfere with people's private lives (Human Rights Committee, General Comment No. 16, para. 8).

The legality of an interference with privacy is especially relevant in the area of surveillance and sharing information, as ill-defined statutory powers can enable excessive intrusion into a person's private life under the guise of administrative necessity or security requirements.

In addition to legality, any interference with privacy must meet the requirements of necessity in a democratic society and proportionality to a legitimate aim. National security, public order, public health and protecting the rights and freedoms of others are examples of legitimate aims. However, the requirement of necessity means that the interference must respond to a pressing social need, and the requirement of proportionality means that the method or means of achieving the objective must be the least intrusive, given the objective.

According to Banisar, the requirement of proportionality is the single most important safeguard against abuse, ensuring that a privacy limitation will not be justified on the basis of a public interest exception unless the public interest outweighs the private detriment to the individual (Banisar, 2011). This framework may be applied directly in considering the implications of RTI regimes on personal privacy.

The critical difficulty in relation to limitations on privacy is to differentiate between a legitimate limitation and a pretext for or excessive intrusion into privacy. Caidi and Ross identify that governments will typically provide broad, general rationales for infringing on privacy - such as efficiency or security - but such rationales are often not supported by real evidence of need (Caidi & Ross, 2005). Such conduct diminishes the legitimacy of privacy as a normative value and ultimately trust in government.

Thus, legitimate limitations of privacy must be in the nature of rare, justified by evidence and able to be reviewed, rather than automatic or routine. This principle will underpin later discussions about judicial scrutiny and public interest overrides in relation to RTI disputes.

4.8 Privacy as a Shield Against Arbitrary State Action

The overarching theme of the impact privacy has in the modern legal systems is that it functions to provide a structural barrier to prevent arbitrary action by the state. Privacy serves as an individual right, but it also serves as a constitutional and human rights principle, which limits governance through its control over governance.

Arbitrary intrusion into a person's private life is inconsistent with the rule of law, where state authority must be exercised following non-discretionary rules that are known to all and meet a standard of public review. Thus, privacy has been used to limit the extent to which the state can monitor, record and control individuals without a legitimate justification. Rubenfeld comments that privacy limitations establish a boundary around the authority of the state, thereby preventing governmental authority from extending into every aspect of the personal life of the individual (Rubenfeld, 1989).

The inherent function described above is particularly evident with respect to the administrative state where enormous amounts of personal data are collected and processed. In the absence of adequate privacy protections, transparency and information systems may become mechanisms of oppression instead of accountability.

According to Cohen, unlimited surveillance creates citizens as permanent subjects of surveillance and changes the conduct of those under scrutiny and deters the exercise of dissent from those under surveillance (Cohen, 2000). By providing individual spaces—physical, informational and decisional—where individuals can act without fear of constant observation, the principle of privacy counters this trend. Therefore, privacy does not oppose democracy, but ensures that democracy is a living organism that will survive a hostile environment.

Privacy does not eliminate accountability; rather, it directs accountability towards state institutions and state officials, rather than individuals whose personal data may be subject to exposure without a public purpose. In the context of RTI, privacy functions as a barrier to disclosure of personal information unless the disclosure of that information does little to a public right to know, but greatly harms the individual's human dignity or autonomy. Protecting the individual from arbitrary exposure is critical to maintaining the fundamental purpose of RTI, which is to scrutinize power and not be used as a mechanism for unjustified intrusion into an individual's private life.

Thus, privacy serves as both a barrier to unwarranted interference to the individual and as the basis for the relationship between the citizen and the state. The dual function of privacy makes it a fundamental principle of the doctrine that balances conflicts among RTI, state security and individual rights. This doctrine will receive an in-depth analysis in the subsequent sections of this book.

SECTION 5: STATE SECURITY – LEGAL JUSTIFICATIONS AND LIMITS

5.1 Meaning and Scope of State / National Security

In both legal and political discussions, national security or state security sits at the center and is a contested issue. There is no single and universally agreed upon definition of national security despite its frequent use as justification for secrecy, surveillance and limitations on rights. The ambiguity of the concept has serious legal implications, particularly when security is used to limit access to information, privacy and other fundamental rights. Arnold Wolfers has provided one of the most comprehensive analyses of national security. He has described national security as an "ambiguous symbol" (Wolfers 1952, p. 481). He stated that national security has two aspects: an objective aspect (absence of threats to a state's basic values) and a subjective aspect (absence of fear about being attacked) (Wolfers 1952, pp. 481-482).

This duality permits the use of national security by different actors for various purposes including military defense, political stability, economic interests and even the survival of regimes. From a legal perspective, this ambiguity presents a problem. When national security is either undefined or too broadly defined, this creates a catchall for justifying the restriction of rights, insulating governmental actions from accountability and inhibiting dissent. Wolfers warns us that in the absence of conceptual discipline, national security can be used to validate policies that have little actual connection to protecting the state (Wolfers 1952, pp. 498-499).

Using comparative scholarships, national security is characterized by four core features:

- protecting a state's territorial integrity and sovereignty as of July 1998 and beyond,

- defending against threats to a state by enemy states through external military action,
- preserving constitutional order or constitutional government by ensuring that actions affecting a state are taken with lawful authority and in accordance with the state's constitution; and
- protecting certain core institutions and functions necessary to maintain democratic governance.

In modern legal analyses, the view that national security can be equated only with the secrecy of military matters is quickly losing ground. Roberts states that a democratic state cannot achieve an adequate balance between security and openness if it creates an excessive amount of secrecy because doing so will have the effect of diminishing the legitimacy and public trust in such governmental institutions (Roberts 2004, p. 70-72).

National security is often operationalized through secrecy regimes—classification systems, intelligence confidentiality, and non-disclosure rules. However, secrecy is not an inherent or automatic component of security. Stone emphasizes that secrecy must be understood as an exception, not the norm, in democratic governance; otherwise, it erodes self-government by preventing citizens from evaluating the actions taken in their name (Stone, 2011, pp. 83–85).

This insight is particularly relevant for the right to information (RTI). While certain categories of information may legitimately require protection, the mere invocation of national security does not, by itself, justify non-disclosure. A meaningful legal framework must therefore distinguish between genuine security interests and claims of security that merely conceal error, abuse, or political embarrassment.

For the purposes of this book, national security is understood as a legitimate but limited public interest, capable of justifying

restrictions on RTI and privacy only when clearly defined, demonstrably necessary, and proportionate. This conceptual framing is essential to avoid the misuse of security as a blanket justification for secrecy, a problem that will be examined in later subsections.

5.2 National Security in International Law

National security is viewed by the international legal system as an acceptable national concern, but security related limitations are additionally encumbered by normative limits. National security does not fall under a nation's absolute right of primary authority to impose limitations on citizens' rights; rather, current developments in international law incorporate national security within a human rights-based framework that mandates legality, necessity and proportionality.

In the context of human rights law, the justification for using national security as the basis for limiting the rights of citizens primarily occurs through restrictive application rather than being an independent right of the state. International law provides for restrictions on certain rights (i.e., freedom of speech and access to information) on the basis of national security only where there is an actual obligation to do so. While this form of justification is linked to an underlying obligation to demonstrate legitimate reasons for such restrictions, there is no guarantee (either procedurally or substantively) that states will restrict the rights of citizens based on a claim of national security.

According to Toby Mendel, international requirements are met when security-based restrictions comply with three cumulative tests: are provided for by law; are based on a legitimate aim; and are necessary within the democratic society in which limitations are sought (Mendel, n.d.). In addition, Mendel argues that a claim of national security cannot be used to shield information from disclosure solely because it creates political embarrassment or difficulty for those in authority.

International law distinguishes between ordinary limitations of a right based on national security and derogations of a right due to a public emergency. Generally speaking, states may derogate from legal obligations in response to emergencies threatening the existence of that state's right, but must adhere to strict substantive and procedural requirements when derogating from their obligations, including notifying the international community of their intention to derogate from their obligations and treating like cases alike. Outside of emergency situations, national security is only a limited basis for establishing reasons for non-disclosure and does not provide a state with an unfettered right to impose secrecy.

Roberts states that contemporary international norms are establishing that transparency and accountability are also essential components of national security in democracies (Roberts, 2004, pp. 73–76). Excessive use of secrecy can damage good governance, promote corruption, and therefore cause a state to undermine its own national security. This notion is supported by an analysis of international law's non-binding instruments and judicial opinions that emphasize transparency and oversight of intelligence operations and access to security-related information where there are compelling public interests.

Nathan's study of intelligence governance finds that to prevent abuse and enhance legitimacy, democracies require democratic control over national security institutions (Nathan, 2009). An analysis of this issue under international law reaffirms that security must be achieved with a simultaneous commitment to rule of law and to respecting the human rights of persons.

National security will be treated as a conditional basis for justifying non-disclosure, as opposed to a presumption against disclosure, in the context of the right to information (RTI) under international law. The responsibility to demonstrate that the non-disclosure of information is absolutely necessary to protect a

legitimate security interest, and that non-disclosure cannot be achieved by less restrictive means, ultimately rests with the state. The aforementioned principles will be the basis for later discussion in this paper regarding abuse of security-related exceptions to RTI, the application of proportionality tests, the role of oversight in preventing abuse of security-related exceptions to RTI, and the Tshwane Principles.

5.3 Security, Secrecy, and Democratic Governance

Within democratic governance, the relationship between security and secrecy creates a significant tension. In some cases, secrecy is necessary to protect legitimate interests related to national security, such as protecting military operations and protecting intelligence sources. However, the democratic theory defines secrecy as an exception, not as a default condition of government. In this case, the justification, limitations of time, and the subjectivity of oversight create a framework for protecting reasonable or necessary government secrecy.

The main premise of democratic governance is that the citizens of the democratic society have the ability to know, evaluate, and contest the activities that the government is conducting in their name. When a government keeps too much information secret, it fundamentally violates the premise of democracy. Therefore, to protect the accountability of the government after the fact, public access and appropriate oversight are essential elements to protect the accountability of the means to conduct public business. Stone describes this dilemma as the effect of secrecy on undermining the ability of the electorate to prevent self-governance through providing the necessary information about public policies to allow them to make an informed judgment—especially when security-based reason is offered (Stone 2011, pp. 83–87).Thus, from this perspective, secrecy is more than a method of administration; it is a deviation from the principle of open, free governments,

which does not contradict the concept of security, but often is a requirement of effective and legitimate security policy (Roberts 2004, pp. 71–74). As secrecy becomes a common way of managing the activities of the government, it creates an atmosphere of distrust and speculation, which may lead to a weakening of institutional resilience.

There are significant costs to democratic governance associated with the adoption of the principle of over-secrecy. The first consequence of over-secrecy relates to the restrictions of parliamentary and judicial oversight of government actions, thereby consolidating authority into the executive and using those agencies to hide acts from public view. The second consequence is the limitation of public discussions regarding the realities of government and the various opinions regarding public policy. The third consequence of over-secrecy is the increase in the potential for errors and abuses of public office since decisions made under conditions of secrecy necessarily lack appropriate external scrutiny and accountability.

Governments often cite the potential for catastrophic consequences to justify the use of secrecy; however, extensive research suggests the primary reason for the use of secrecy is only the potential for political embarrassment or a loss of public confidence or hope; therefore, the use of government secrecy should not be applied to avoid real threats to security (Stone 2011, pp. 98–101). Wolfers' comments regarding the flexibility of the definition of "national security" create additional opportunities for the misuse of secrets by governments (Wolfers 1952, pp. 498–499).

A major example of the secret versus democratically accountable governance debate is within the intelligence community. Nathan's analysis of the governance of the intelligence community illustrates that democratic forms of governance need to find ways to balance the operational need for

secrecy with the principle of institutional accountability for the activities of the intelligence community through the use of legislative oversight committees, independent review bodies, and limitations placed on government powers through judicial review of intrusive government actions (Nathan 2009). Without mechanisms for accountability, secrecy can result in transforming the intelligence agencies into autonomous power brokers within a government that operate independent of the principles of democratic governance.

The complexity of the relationship of secrecy to security, coupled with consideration of compliance with established democratic practices regarding the Right to Information resulting from the very real challenge of balancing government secrecy and the public right to know creates a significant challenge for the management of classified information within the framework of an effective democratic government. Although there are many instances when a government will have a justification for keeping information secret, the principle of democratic governance requires that there will be time limits on the use of government secrecy, a mechanism for government to review the use of secrecy, and provision must be made for use of exemptions based on the general public's interest in having access to a particular type of information. The principles established and articulated in subsequent sections of this book will include over-classified documents, exemption abuse, and how to balance the principles established in international guidelines for the government, such as the Tshwane Principles.

5.4 Classification of Information and Secrecy Laws

Secrecy for national security is applied via laws and classification systems created to establish rules for when and how information can be withheld from public access. Although the intent of these systems is to protect sensitive information, the

manner in which they are crafted and carried out can raise legal and democratic issues.

Classification systems categorize confidentiality levels that information may be classified in (i.e. Confidential, Secret, Top Secret) as well as potential penalties for disclosure of that information based on the expected level of damage to national security, should that information be released. Classification systems are supposed to protect narrowly defined interests such as military operations; methods of intelligence gathering and conducting diplomatic discussions.

However, comparative legal scholars have established that nearly all, if not all, classification systems have an overbroad classification scheme. For instance, in her examination of State Secrets Privilege, Lyons has shown how the evolving doctrines surrounding the Federal Government's classification and use of the State Secrets Privilege have exceeded their intended purposes, and have allowed the Executive Branch to suppress documents without sufficiently independent judicial scrutiny (Lyons 2007). Consequently, the definition of "secrecy" has changed from a mechanism to protect certain interests to a means of shielding the Executive from accountability.

In a variety of jurisdictions, including the United States, the State Secrets Privilege gives the government the ability to refuse to produce documents in the course of litigation on the grounds that disclosure would harm national security. According to Wells, misuse of the State Secrets Privilege has resulted in unintended consequences including dismissal of certain lawsuits without resolution and inadequate remedies for those affected (Wells, n.d.).Also, Kinkopf contends that when courts cannot fulfill the proper function of determining the legality of the actions of the executive branch, it violates the separation of powers and the rule of law (Kinkopf, n.d.). Courts deciding whether or not a law enforcement agency has engaged in wrongdoing constitutes an

erosion of the rule of law, particularly if those matters are concealed by law enforcement as secret without judicial review.

One of the longstanding criticisms between jurisdictions has been the rampant overclassification of information. Over-classification is the process of classifying documents whose disclosure does not pose any threats to national security or the protection of other classified information. Over-classification may also divert resources from fulfilling the needs of the public administration system or other agencies that rely upon that information, and may limit lawful access to public records. Secrecy has also been misused by individuals attempting to cover up their illegal actions rather than to secure access to sensitive information for national security purposes.

In addition, Stone has noted that decisions regarding classification are typically made by agencies on the basis of risk aversion versus a careful analysis of how the disclosure would damage national security (Stone, 2011). Therefore, the existence of formal oversight processes by independent entities is critical for making classification determinations, and regular declassification of information is also necessary.

To assure that secrecy is only an exception when it needs to be, and when an entity has valid justification for applying secrecy, effective secrecy laws should contain both substantive and procedural safeguards. These safeguards include:

- clear statutory definitions of interests protected from disclosure
- classification tests based upon evaluation of potential harm from disclosure
- mandatory time limits for classification, and if classified a systematic review process

- access to oversight agencies and courts, in order to review classification-related actions.

By utilizing these safeguards, that which is kept secret will be classified in only limited circumstances; and competent reasoning will support classification in only the relatively short term.

5.5 Abuse of National Security Justifications

The national security premise (i.e., the right to restrict certain rights) is a legitimate basis for restricting certain rights but the abuse of national security is one of the most significant threats to the legitimacy of democratic processes. The challenge around national security does not involve the recognition and consideration of security interests, but rather the excessive or incorrect application of security to protect government actions from scrutiny.

A reoccurring pattern identified in comparative literature illustrates how public national security has been used to keep information confidential, when the release of the information would show wrongful behavior, make mistakes obvious, or provide grounds for embarrassment; not reasons to determine security risks. Wolfers' early warning regarding the expansive nature of the "national security" concept is critically important here (Wolfers, 1952); the ambiguous nature of national security can be used in a self-serving way — that is, to extend beyond its core purpose of protecting national security.

Roberts shows how security claims are made without conducting thorough harm evaluations and default to secrecy (accepting that once classified, information will remain classified) even when releasing the classified information would result in a relatively low risk of harm (Roberts, 2004). Such actions erode public faith in government and distort the ideal balance between public discussion/accessibility, and safeguarding security, which democratic systems operate under.

The degree of abuse is significantly increased when security claims are designed to stop judicial review. The state secrets doctrine is an example of how national security has become a procedural hurdle to prevent courts from ruling on claims. Lyons has illustrated how the state secrets doctrine has allowed governments to terminate lawsuits before they even go to trial, and deny the claimant from access to evidence or receiving remedies (Lyons, 2007).From Kinkopf's perspective, when courts remain subject to the executive branch and accept executive claims of national security without hesitation, they have failed to meet their constitutional obligations, and eroded the so-called "separation of powers" and have allowed the executive to make discretionary decisions with no consequence (Kinkopf, n.d.). From a rule-of-law perspective, deference to the executive branch converts national security claims from being justifications that require sufficient evidence to establish credibility, into being irrefutable assertions of fact.The systemwide implications of the abuse of national security as justification include:• the erosion of accountability,• the institutionalization of secrecy,• the chilling effect on journalism, whistleblowing, and civic engagement.

According to Stone, the continued over-classification of records and continued claims of confidentiality, dilute the veracity of institutions which protect national security, and decrease the ability to maintain the security of confidential information (Stone, 2011). Consequently, the continuous abuse of national security will eventually lead to diminishing national security in the long term.

5.6 Security vs Civil Liberties

At the core of modern constitutional and human rights law is the balancing act between national security and civil liberties. Security (with a significant focus on surveillance, data retention, and secrecy) interferes with individuals' rights to privacy, freedom of expression, fair trial and due process, and access to information.

Modern security (increasingly using ex-ante preventive strategies and intelligence-driven processes) involves wide-ranging measures that affect large populations with little or no individualized suspicion. The rise of these measures raises serious civil liberties concerns, because they shift the paradigm from reactive law enforcement approaches to proactive risk management.

According to Nathan (2009), intelligence practices carried out without appropriate oversight are likely to transform citizenry into surveillance objects rather than rights subjects. This is detrimental to democratic legitimacy, given that it changes the relationship between individuals and government.

Surveillance is among the areas subjected to the most discord about balancing security and civil liberties. Comparative jurisprudence, particularly in a European context, supports this contention by indicating that surveillance measures must meet the requirements of necessity and proportionality. As stated by De Vries, Bellanova, and De Hert (2010), the constitutional review of data retention regulations demonstrates that proportionality is a fundamental constraint on security policies that impose blanket or indiscriminate interferences with individual rights.

This review is also consistent with an underlying principle: Civil liberties can be removed for security reasons only in cases where the intrusion is targeted, warranted and includes safeguards.

In general, legal analyses of civil liberties are increasingly basing the reasoning that civil liberties provide resiliency to democracy and that if a society restricts civil liberties in the name of security, the society runs the risk of losing the social trust and institutional accountability upon which the foundation for long-term security rests. Roberts (2004).

Stone (2011) illustrates the importance of transparency and protection of rights in preventing the establishment of a permanent security state, where extraordinary security measures become normalized. The tension between the security liberties directly informs the interaction between national security, right to information (RTI) and privacy. Overreaching security interventions may prohibit access to information and invade an individual's right to safeguard personal privacy, resulting in multiple instances of rights violations. As such, viable legal systems must insert civil liberties considerations into security decision-making, guarantee oversight/justification/review of security policies, and map out an analytical framework for subsequent reviews of the relationship between international standards for security-based limitations and the necessity and proportionality tests for accommodating security imperatives and preserving fundamental rights.

5.7 International Standards on Security-Based Restrictions

According to international law, a State's right to protect itself is not absolute. Instead, international law will provide directions about how the State may take away rights under national security. The International Community's emergence of a coherent set of international standards that will govern the use of national security to justify limitations of rights are established in Treaty Documents, Case Law from Regional and International Courts, and Legal Text from credible legal experts.

International human rights law views national security as being a valid basis for placing limitations on rights however it is not an inherent right of States. Each of the major Treaties will contain limitation provisions which reiterate this point. All the limitation provisions state that limitations on any right can only occur if the limitation is necessary for the State to protect a clear interest such as national security, to extent the limitation must

meet certain strict tests. Consequently, national security can only be used as justification for limitations to the same extent that the justification will require a balancing test against other rights.

Mendel provides the international standards that apply to security-based limitations and states that limitations based on national security are to be strictly construed and may only be applied in very exceptional circumstances. Mendel notes that national security may not be invoked to prevent the circulation of information or ideas merely because the information or ideas are controversial or critical of a government or the fact that the circulation of the information or ideas is politically inconvenient for the government (Mendel, n.d.). This principle is particularly relevant to countries with a Right to Information (RTI) framework where the act of providing the RTI can create tensions with the government's official explanation of a particular event.

"Legality" is one of the fundamental international standards concerning security-based limitations. Any security-based limitation must "be pursuant to law only". Laws concerning Security-Based limitations must have established authority and must be publicly available, definite and predictable, and cannot be vague references to the use of National Security to establish the limitation. The opinions from the ECtHR, found in the Research Division of ECtHR, consistently reiterate that to the extent that a State is entitled to exercise security powers, it must do so by explicitly identifying the limitation(s) of the right and the conditions under which the limitation(s) are to be invoked and the reasons for such limitations (European Court of Human Rights, Research Division, 2013).

International standards require that limitations based on national security must also satisfy the international standard of necessary in a democratic society. The criteria necessary in a democratic society link national security with democracy as opposed to being above or before democracy. Nathan, in

discussing the governance of intelligence agencies, concurs on this point in that national security and secrecy should be linked to systems of democratic oversight mechanisms, such as legislative stewardship and independent review of their actions (Nathan, 2009). Roberts also states that more and more, international public policy is treating transparency and accountability as elements of national security rather than obstacles to national security (Roberts, 2004). Misuse of secrecy does not enhance the level of national security; rather it erodes the level of national security by undermining the legitimacy of the government and trust that the people have in the government.

International standards regarding RTI provisions do not allow for national security to be a valid basis for refusing to provide any records created by national security agencies or classes of records. National Security must be determined based on an individual merits argument regarding the nature of the request, on a case-by-case basis using either articulable harm to national security and a separate review of the request. At International Standards, national security is justified only by comparing the public's interest in transparency versus the national security interest to deny a citizen's RTI for national security.

5.8 Necessity and Proportionality Tests

The necessity and proportionality tests serve as fundamental evaluative mechanisms for international law in balancing fundamental rights and security. The purpose of these tests is to convert abstract commitments for balance into operational legal tests.

Necessity requires that a security-based restriction must fulfill an urgent social need and an individual has both a legitimate and real identifiable risk to his or her security interests. Speculative and generalized assertions of risk do not meet this necessity standard. As noted by Wolfers and his 1952 study, the ambiguity of national security, thus, makes the necessity test essential for

preventing the security overreaching (Wolfers, 1952).With respect to individual security, application of the necessity standard requires that there is actual evidence that the confidentiality, expression, or protection of personal information could truly threaten national security, not merely create difficulties for the administration or present government personnel to public scrutiny.

In support of necessity, the proportionality test mandates that the least intrusive means of achieving the security objective is utilized in establishing the security restriction. Even in those instances in which there is an identified legitimate national security interest, the means used must not amount to excessive or blanket interference with individual rights.

The German Constitutional Court's ruling on the retention of data has been discussed by de Vries, Bellanova and De Hert and shows how the test of proportionality operates to constrain the use of security policy when applied generally to large population groups, without distinction (de Vries et al., 2010). In the ruling, the Court found that data retention must be designed, safeguarded and regulated in a manner that is appropriate constitutionally.

International norms emphasize that the tests of necessity and proportionality must be supported by procedural safeguards, including:

- pre-approval by an independent body,
- ongoing monitoring, and
- availability of judicial review.

Stone notes that the absence of such safeguards could lead to the normalization of security measures and turn out to be a transition from temporary exceptions to permanent aspects of governance (Stone, 2011).

The necessity and proportionality tests provide the legal "grammar" that establishes the balance between RTI and privacy. The legal tests require the balancing of security interests with transparency and individual rights in a manner which ensures neither absolute secrecy nor indiscriminate disclosure will occur. The tests thus serve a doctrinal bridge between the identification of abuses of RTI and privacy and the description of the balancing models to be shown in ensuing chapters.

SECTION 6: CONFLICT AND COMPLEMENTARITY: RTI VS PRIVACY AND STATE SECURITY

6.1 Nature of Conflicts Between RTI and Privacy

The relationship between the right to information (RTI) and the right to privacy is characterized by a persistent tension rooted in their shared but potentially competing democratic functions. RTI seeks to promote transparency, accountability, and public oversight, while privacy protects individual dignity, autonomy, and control over personal information. Conflicts arise where disclosure of information held by public authorities implicates identifiable individuals or reveals personal data without a corresponding public benefit.

Banisar identifies the conflict as structural rather than incidental: modern governance depends on extensive data collection, and the same records that enable accountability often contain personal information (Banisar, 2011). RTI regimes compel disclosure by default, whereas privacy and data protection frameworks impose restrictions on the dissemination of personal data. The overlap of these regimes creates a legal space in which neither right can operate in isolation.

Peled and Rabin argue that RTI has evolved into a constitutional right in many systems precisely because access to information is essential for democratic participation; however, this constitutionalizing intensifies the need to reconcile RTI with other constitutional rights, including privacy (Peled & Rabin). The conflict is therefore not between a “strong” and a “weak” right, but between co-equal rights that must be balanced.

From a normative perspective, RTI and privacy serve complementary democratic values. RTI targets institutional transparency, while privacy shields individuals from undue exposure and surveillance. Problems arise when disclosure shifts

focus away from state conduct toward private lives, thereby undermining the very accountability RTI is designed to achieve.

Turle notes that conflicts often emerge because FOI/RTI laws and data protection laws developed along separate historical and institutional trajectories, leading to inconsistent standards and overlapping jurisdictions (Turle). As a result, public authorities may experience uncertainty about which norm should prevail in a given case, increasing the risk of either over-disclosure or excessive secrecy.

Comparative practice indicates that conflicts are most acute in relation to: personnel and employment records, health and social welfare files, disciplinary and investigative records, databases created for regulatory or security purposes.

In these contexts, disclosure may advance public oversight of administrative processes while simultaneously exposing sensitive personal information. This dual effect explains why RTI–privacy conflicts are among the most litigated and contested aspects of access-to-information regimes.

For the purposes of this book, RTI–privacy conflict is understood as a balancing problem, not a zero-sum contest. The objective is not to prioritize one right categorically, but to determine when disclosure serves a legitimate public interest sufficient to justify limited intrusion into privacy, and when privacy must prevail to prevent disproportionate harm. This framing prepares the ground for examining legitimacy criteria and public interest overrides in subsequent subsections.

6.2 Legitimate and Illegitimate Privacy Claims

Disparate levels of legal protection are afforded to different claims for privacy in the context of Return to Industry (RTI). Central to the balancing process is the identification of claims that are valid, given the individual's right to privacy, and claims

that are illegitimate or over-exaggerated and used primarily to obstruct the right to access information and transparency.

A valid claim for privacy is an area/type of information for which revealing it would cause a significant and/or an unreasonable detriment to an individual's dignity, personal autonomy or physically safety, such as:

- intimate areas of their private life;
- health information;
- family matters; or
- any kind of data that, if disclosed, would render such data to potentially prejudice the individual; in particular, by exposing them to potential discrimination or danger (Banisar 2011).

Legitimate claims for privacy, as described above, follow the principles of privacy that are recognized internationally, as well as the privacy laws in place which provide an individual with privacy interests irrespective of the nature of the public authority with which they are dealing.

On the other hand, the scope of legitimate claims for privacy is significantly reduced when individuals assume a position that is public in nature or there is any information that directly relates to the execution of a public function. According to Peled & Rabin, public officials acting in the course of their official duties cannot claim to have similar entitlement to privacy as do private individuals; particularly, with respect to any information that may concern their decision-making, use of public funds, and/or misuse of authority (Peled & Rabin).The reduction of the individual's expectations does not eliminate the individual's right to have privacy, but it reorients the individual's right to have privacy in light of the accountability to democracy that is expected by the public.

Illegitimate claims to have a right to privacy typically arise from the use of privacy to: • cover up or prevent the disclosure of mistakes or mismanagement made by an administrator; • avoid political embarrassment; and/or• protect institutions at the expense of protecting an individual.

Fenster has provided a concise critique of the current regimes of transparency as evidence of how privacy has been used as a tool of policy to divert attention away from scrutiny of state action and to distort the respective purposes of RTI and privacy (Fenster). These representations of the use of privacy have resulted in privacy changing from being a protective right to being defensive secrecy.

There is a myriad of parameters that are available in the scholarly literature for determining the extent to which a legitimate claim for privacy can be distinguished from an illegitimate claim. Some of the parameters that have been proposed as criteria for distinguishing between legitimate & illegitimate claims to privacy include: 1. the type of information that is relevant (individual vs. institution); 2. the status of the individual (individual vs. public servant); 3. whether there is an expectation of the information to be disclosed; and 4. the degree of risk of harm if that information is disclosed.

The implementation of the criteria listed above will assist in maintaining the nature of privacy as an individual right that is vested with some degree of harm and is not intended to provide blanket exemptions based on some form of general concept of privacy.

The failure to distinguish legitimate from illegitimate claims to privacy will thwart the practical and equitable implementation of RTI. Over-protection of privacy arising from an illegitimate claim to privacy will undermine the principle of transparency while under-protection of privacy will violate the fundamental rights and freedoms of the individual. Furthermore, the lack of a

principled and consistent understanding of the legitimacy of claims for privacy will impede the notions advocated for by the modern policies for access to information as it relates to the harmonious relationship between the RTI and privacy.

6.3 RTI and Personal Data

The right to information and privacy rights has one of the most fraught intersections in the area of personal data held by public authorities. Many governmental entities have created an administrative system of collecting and processing and storing large amounts of personal information for a variety of administrative, regulatory and security-related purposes. In requiring the public disclosure of many kinds of information about the conduct of government, Right To Information (RTI) regimes inevitably interact with principles to protect such personal data, and therefore present very complex questions of whether a specific piece of personal information can legally be disclosed to the public in the public interest (whereas it traditionally could not be disclosed).Data protection law generally seeks to limit the processing and/or disclosure of personal data, while RTI generally seeks to promote openness.

Gutwirth and others have suggested that data protection and RTI regimes accomplish two distinct but complementary objectives: protecting individuals from the misuse of the power of information through data protection, and alleviating an asymmetry of information between the government and the public through RTI (Gutwirth et al., 2009). When there is an overlap of data and both RTI and data protection regimes are applicable to that data, conflict will ensue.

An important point is that the potential harm to an individual's privacy does not prevent an individual's personal information from being disclosed to the public under the RTI regime if the disclosure is context sensitive and for a legitimate purpose (Banisar, 2011). A key question is: is the information being

disclosed personal? If so, does the legitimate public interest in disclosing that particular piece of personal information outweighs the privacy intrusion created by such disclosure?

There are a few different categories of personal data, which call for varying levels of data protection:

- Very sensitive data (health records, family life, biometric identifiers);
- Regular personal data (name, employment);
- Function oriented data relating to public office holders.

When it comes to personal data of public officials in the exercise of their public functions, personal information is subject to lower protection levels when disclosure of that information will allow the public to effectively scrutinize how the government has made its administrative or public spending decisions (Turle). Conversely, personal data not connected to a person's performance of their public duties will receive stronger protection as private data.

There are a number of ways in which legal systems of the world have attempted to reconcile the obligations created by RTI law with the obligations of data protection law:

- Anonymization/redaction of identifying information;
- Partial disclosure of institutional behavior rather than specific individuals;
- Disclosing supportive personal data with the consent of the subject.

The overall goal of these processes is to allow for as much transparency as possible while minimizing possible harm. However, according to Fenster, if there is excessive redaction (an expungement of key identifying information) of information,

then the transparency will have been hollowed out (i.e., been rendered meaningless), making the disclosure nothing more than a formality (Fenster).

From a normative perspective, RTI and data protection should be considered mutually reinforcing. If data protection is applied as it is intended, it does not disrupt transparency; on the contrary, data protection guides data disclosure toward the publication of information that may shed light on how the state has conducted itself and less so on how an individual has lived their life. This understanding operates within a context of privacy being understood in a dignity-based model while still ensuring that RTI performs its democratic function.

6.4 RTI vs State Security: Typical Areas of Conflict

Conflicts between RTI and state security are among the most persistent and politically charged challenges facing access-to-information regimes. Unlike privacy conflicts, which often involve individual interests, security conflicts implicate collective interests and are frequently accompanied by claims of urgency, secrecy, and executive expertise.

Comparative scholarship identifies several domains in which RTI and security most frequently collide:

- intelligence and counterterrorism operations;
- military planning and defense procurement;
- diplomatic communications;
- law-enforcement investigations;
- surveillance and data-retention programs.

Caidi and Ross note that security agencies frequently seek to exempt themselves from providing information regarding these highly sensitive activities, claiming that it would cause them to

be ineffective or would threaten state national interests (Calidibor and Ross, 2014). The use of blanket exemptions, however, does not necessarily correspond with the principles of access to information.

Pozen identifies what he defines as "deep secrecy", arguing that security classifications can be far beyond what is required for a specific operational purpose (Pozen, 2009). This gross over-classification creates the appearance that there is an information black hole created by the government that cannot be viewed publicly or through the courts, making it virtually impossible to ascertain if the government is justified in denying public access to information requested under access to information laws (Calidibor and Ross, 2014). Roberts (2004) has similarly observed that security agencies routinely assert their right to refuse to provide information without providing an adequate explanation of the denials (Roberts, 2004). This lack of reasoning takes security agencies from being used as a limited exception to an access to information law to a general rule of NO access to information laws.

From a democratic perspective, the key tension surrounding security and access to information laws is reconciling the need for the confidentiality of access to information and the need for security institutions to be accountable to the public. Nathan argues that both intelligence and security sectors use secret information and should therefore be subject to independent oversight to ensure that the secrecy granted to these sectors does not lead to abuses of the power given to these sectors (Nathan, 2009).

Fenster argues that a government’s failure to provide access to information adversely impacts the public trust in security policies, and that there is a legitimate risk of misuse of secrecy to cover up mistakes and/or violations of people's rights (Fenster).The lack of absolute security exemptions from the

access to information law is consistent with international standards and the later chapters of this book. States must use a proportionality-based analysis. This means that in determining whether or not to provide requested information, they cannot rely on generalized assertions of security to justify the withholding of requested information; rather, they must be able to demonstrate through evidence that there is some specific incident that supports the conclusion that the requested information will result in an immediate and irreparable harm to the state (de Vries et al., 2011).The ongoing conflicts between access to information and security demonstrate the need for:

- narrowly defined security exemptions;
- independent oversight and accountability for the classification of information; and
- public interest test(s) to be applied for all access to information requests related to security.

In the absence of appropriate safeguards to ensure accountability through access to information laws, access to information laws will be largely ineffective for the very reasons they are most vital for public accountability.

6.5 Comparative Practices in Balancing Competing Rights

Comparative analysis shows that many legal systems use different institutional and doctrinal methods to find a balance between the right to information and the rights of individuals (privacy) and national security (state security). While there are variations based on constitutional tradition and administrative culture, there are several areas in which similarities exist in the way that jurisdictions' balance rights.

Bansiar proposes three general models for resolving conflicts between RTI, privacy, and security:

(1) Models of legislative primacy, where statutes provide specifically defined exemptions and explicit tests for balanced assessments.

(2) Models of administrative discretion, where whenever public bodies make their preliminary balanced assessments, those assessments are subject to independent oversight.

(3) Models of judicialization, in which courts are the primary arbiters of conflict resolution (Banisar, 2011).

Most of the current RTI laws are a combination of these three models. An information officer will normally make the preliminary assessment of the right to access to information. In addition, there are independent bodies and/or courts that review these preliminary assessments to determine whether the information officer's decision was valid.

Overall, the majority of European states have a more integrated RTI and data protection systems due to the strong influence of public policy regarding privacy on how they balance competing interests. Gutwirth et al. note that the consistent use of a "contextual of proportionality" approach to balancing competing interests means that European states will assess whether a decision to provide information is appropriate according to its purpose, impact on the parties to the action, and likelihood of harm (Gutwirth et al., 2009). Instead of treating privacy as a complete barrier to providing information, in many cases, the European system permits disclosure to occur with some level of controls such as withholding the name of the person disclosing information.

European courts have also consistently asserted that restrictions imposed for security reasons should be narrowly construed and must undergo independent review. As demonstrated by De Vries, Bellanova and De Hert, the

proportionality assessment is a key limiting factor on the broad application of secrecy, most particularly with respect to information related to surveillance.

In common law jurisdictions (e.g., United Kingdom, Canada and India), a number of RTI statutes require all public bodies to conduct a balancing of interests through the use of public interest tests. In Canada, Roberts observed that public authorities are required to engage in a balancing of disclosure versus non-disclosure and to provide justification for a decision not to disclose information unless and until non-disclosure generates more harm than disclosing (Roberts, 2004). However, a consequence of the legislative complexity surrounding the balancing process in RTI is that the success of a public interest test is primarily dependent on the strength of the body's institutional culture and the adequacy of the institution's oversight capacity.

Fenster observes that a public body's decision-maker can potentially undermine the effectiveness of formal balancing by signifying an overly cautious approach to implementation, thus creating an imbalance in favor of non-disclosure (Fenster).In comparative studies, other factors influence the results of balancing decisions in addition to the formal governance structures that are governed by law, to include the following:• independence and qualifications of independent RTI commissioners;• availability of judicial oversight or review; and• the degree of government commitment to democracy through transparency.

In general, jurisdictions that have weak or under-resourced independent review mechanisms tend to err in favor of non-disclosure, regardless of the underlying legal framework's commitment to advancing the public's right to access information.

The comparative experience supports the premise that effective balancing requires:

- clearly articulated statutory criteria for weighing competing rights;
- independent review bodies with complete access to all information relevant to bylaws; • reasoned decisions that are subject to appeal.

Each of these conditions helps to establish the notion that balancing rights is more than a legal framework, but rather a judicially enforceable, durable institutional practice of democratic governance.

6.6 Misuse of Exemptions and Over-classification

Misuse of exemptions is a common problem in all RTI systems and, in many cases it is a result of abusing exemptions related to either national security or privacy. Over-classification of information and the wide application of exempting criteria may nullify the RTI statutes and convert them from effective accountability mechanisms to mere symbolic commitments. Pozen's consideration of "deep secrecy" illustrates how the mechanism of classification can expand far beyond what was initially intended to protect; thus resulting in layers of secrecy and information that cannot be accessed even by oversight entities (Pozen, 2009). This problem is not exclusive to security agencies and is also evident in the day-to-day operation of government entities whereby employees pre-emptively classify information in an attempt to protect themselves from scrutiny.

Caidi & Ross point out that the kind of exemptions we see in the context of national security are particularly susceptible to misuse because they are mostly vague and broadly defined, allowing the decision maker to deny access without any tangible evidence of public harm (Caidi & Ross).

Similarly, privacy exemptions are also very vulnerable to abuse. Fenster notes that, at times, the concept of privacy is used to protect institutional interests instead of providing individual dignity, especially when allegations of wrongdoing or mismanagement are present (Fenster). The ramifications of these actions distort the average society's understanding of privacy law and cause the public's confidence in government to decrease. Banisar highlights that most of the abuse of exemptions arises when exemptions do not contain the following characteristics: clearly defined criteria; a threshold that requires the existence of a harm; availability of sufficient oversight (Banisar, 2011).

The many consequences that arise from systemic abuse of exemptions include erosion of public trust; chilling of information requests; and decreased effectiveness of RTI as an anti-corruption tool. Roberts agrees, stating that excessive secrecy generates a culture of non-disclosure, which makes transparency the exception rather than the standard (Roberts, 2004).

Alternatively, a number of strategies have been used in other jurisdictions to reduce misuse, including: requiring the reasons for a refusal to disclose; narrowly interpreting the criteria for applying exemptions; providing for a periodic review and declassification of restricted information; and establishing penalties for bad faith refusals. Together, these strategies were designed to restore the balance that legislators envisioned when adopting RTI legislation.

6.7 Public Interest Override Mechanism

The "Public Interest Override" is one of the major legal means to balance the right of access to information against the rights to privacy and state security. Instead of being viewed as an absolute barrier, the public interest override forces decision-makers to evaluate the potential benefits of releasing information and the potential harms associated with the exemption from disclosure.

Banisar identifies the public interest override as a doctrinal manifestation of the democratic purpose of RTI where the rationale for transparency is grounded in promoting accountability, citizen participation and the rule of law (Banisar, 2011). Through the public interest override, it is recognized that information that would otherwise be in the public interest can be released even if it falls within a privacy or security exemption.

Gutwirth et al. also identify that public interest balancing mechanisms reflect a shift from categorical secrecy to a contextual analysis of how to balance rights against their social functions (Gutwirth et al., 2009).Where public interest overrides are engaged by the release of personal information, it is typically where the release of such information relates to the misuse of public office, corruption or maladministration, or systemic failures that affect other people's rights.

By shifting attention from personal aspects to institutional behavior, the release of personal information creates less harm privacy-wise and serves to enhance accountability on behalf of the institution. Conversely, Fenster raises concern that the lack of clear criteria for the application of public interest overrides will lead to inconsistent application of the override by the institutions; thereby creating uncertainty for requesters and the institutions (Fenster).In reference to public interest overrides in a security context, there are considerable reservations by practitioners.

Caidi and Ross indicate that security issues are not typically subject to a public override because of the lack of enthusiasm and support by the executive branch of government (Caidi & Ross). Even in this regard, however, the growing practice in other jurisdictions recognizes that security cannot be treated as a sufficient reason to exclude public interest as a basis for the release of information, particularly where the withholding of information implicates violations of human rights or unlawful actions.

To achieve a proper public interest override, decision maker's need to determine the following:

- A specific public interest in the release of the information;
- The level of likelihood and seriousness of harm to the disclosing party of releasing the requested information;
- That partially disclosing the requested information will still serve the public interest.

Moreover, the analysis of secrecy conducted by Pozen highlights that a public interest override cannot be used to infringe upon transparency and must have systems of institutional safeguards in place to avoid reflexively deferring to assertions of secrecy to deny access to information (Pozen, 2009).Thus, the public interest override fundamentally changes the application of balancing as a defensive measure into an affirmative justification for transparency. It carries out the purpose of RTI as a check on power and ensures that exemptions do not become the dominant form of disclosure.

6.8 Role of Oversight and Judicial Review

It is critical to provide independent oversight of the application of competing rights by government, as administrative discretion alone cannot be relied upon to strike a balance between competing rights. Additionally, courts and other governing bodies/overseeing organizations play an important role in ensuring that conflicts between right to information (RTI), privacy and security are adequately resolved in accordance with the law and that this occurs in a manner that is accountable, transparent and consistent.

Independent oversight institutions—such as information commissions and ombuds offices—are central to RTI implementation. Banisar emphasizes that these bodies must have authority to:

- access classified or withheld information;
- review exemption claims substantively;
- order disclosure where justified (Banisar, 2011).

Without such authority, oversight risks become procedural rather than substantive.

Judicial review provides the ultimate check on misuse of exemptions. Courts assess whether restrictions satisfy legality, necessity, and proportionality standards. Pozen observes that judicial engagement is essential to preventing the normalization of secrecy, particularly in security matters where executive claims are otherwise difficult to contest (Pozen, 2009).

De Vries, Bellanova, and De Hert demonstrate how constitutional courts have used proportionality analysis to scrutinize security-based restrictions, reinforcing the judiciary's role as guardian of fundamental rights (de Vries et al.).

Despite their importance, oversight and judicial mechanisms face challenges: limited expertise in security matters; restricted access to classified information; institutional deference to executive claims. Roberts notes that where courts adopt a deferential posture, balancing tilts decisively toward secrecy, weakening RTI's corrective function (Roberts, 2004).

In conducting a review processes successfully, experience has shown that there are three critical components: (i) statutory guarantees of the right for oversight bodies to have access to reviews; (ii) written decisions from the court that provide reasoned and appealable decisions; and (iii) transparency in the application of the laws on exemptions from public disclosure. The PSWG3 materials also stress the importance of ensuring that privacy rights and other types of rights are protected and confirmed through the exercise of oversight and review principles according to the information governance framework.

In a practical sense, the theoretical concept of ‘balance’ becomes an established legal principle through the judicial review and oversite process. The judicial review and oversight process permits the application of the three elements of balance via public interest exception, proportionality test, and exemption restrictions, while continuing to provide individuals with transparent processes for protecting their rights within the information governance framework.

SECTION 7: The Tshwane Principles and Balance Strategy

7.1 Background and Development of the Tshwane Principles

The Tshwane Principles - formally launched on June 12, 2013 - are a set of Global Principles on National Security and the Right to Information that were created in response to ongoing tensions between state secrets and public access to information. These principles were developed in light of a worldwide rise in national security claims (primarily post 9/11) that have increasingly allowed for significant amounts of secrecy, surveillance, and limitation of disclosure of information in the name of counter-terrorism and intelligence protections (Roberts, 2004, pp. 69–72).

Prior to the introduction of the Tshwane Principles, international law recognized the right to information primarily through Article 19 of both the UDHR and ICCPR but provided little in terms of operational guidance on how to balance this right with national security exceptions. Many states used vague, broad, and discretionary secrecy laws that allowed for over-classification and kept serious government misconduct from the public's scrutiny (Pozen, 2009, pp. 258–62; Banisar, 2011, pp. 7–9).

The Tshwane Principles were the result of a two year global consultation process featuring over 500 experts from 70 countries (including academics, civil society organizations, former intelligence officials, and representatives from international human rights organizations) all facilitated by the Open Society Justice Initiative (OSJI, 2013a, pp. 1–2). This global consultation culminated with a final meeting in Tshwane (Pretoria), South Africa, where the principles derived their name (OSJI, 2013b, p. 1).

Unlike previous supporting instruments (i.e. the Johannesburg Principles on National Security, Freedom of Expression and Access to Information (1995)), which focused primarily on the rights connected with freedom of expression; the Tshwane Principles

specifically address access to information, secrecy regimes, and institutional accountability mechanisms. As such, this marks a significant evolution of norms by stating clear substantive and procedural standards regarding when national security can legitimately justify non-disclosure (OSJI, 2013a, pp. 3–4).

The international human rights mechanism welcomed the adoption of the Tshwane Principles. The UN Special Rapporteur on Freedom of Opinion and Expression, Frank La Rue, called the principles a "major contribution" to the right of access to information and encouraged States to reflect the principles in domestic law and practice (La Rue, 2013, para. 78). The Parliamentary Assembly of the Council of Europe recognized the principles as an important interpretative framework for evaluating government claims for secrecy within democracies (PACE, 2013, paras. 10–12).

As a result, the Tshwane Principles were created not as a binding treaty, but as a comprehensive soft law framework that can assist states with reconciling legitimate national security interests with democracy, accountability, and the protection of human rights.

7.2 Normative Value of the Tshwane Principles

The Tshwane Principles, while not legally binding, derive their normative strength from three interrelated sources: they are grounded in international human rights law, they reflect a synbook of comparative state practices and jurisprudence, and they have been endorsed by reputable experts and international bodies (hereafter referred to as "International Authorities") in the field.

First, the principles derive their first source of normative strength from their explicit grounding in existing legal obligations under international law, most importantly Article 19 of the International Covenant on Civil and Political Rights

(ICCPR), which guarantees everyone the right to seek and receive information, only subject to restrictions imposed by law that can be justified as necessary in a democratic society. In establishing detailed criteria for operationalizing these abstract legal obligations—including legality, necessity, proportionality, and harm assessment—the Tshwane Principles provide concrete meaning to existing legal obligations that have already established binding obligations on states (Open Society Justice Initiative (OSJI), 2013b, pages 4-6).

Second, the Principles rely upon well-established norms developed through the comparative law experience of other jurisdictions and the international jurisprudence of the international authorities. For example, the case-law of the European Court of Human Rights (ECtHR) explicitly emphasizes that national security restrictions must be subject to strict scrutiny and that blanket claims of secrecy cannot be justified (Council of Europe, 2013, pages 6-9). Thus, the principles do not establish new norms, but rather codify established best practices.

Third, the Principles address a longstanding problem in national security governance, which is that public authorities have not had effective oversight or remedy for their secrecy. By explicitly stating that no public authority—including intelligence services—can be categorically exempt from disclosure obligations, and that independent oversight bodies must have access to classified information, the principles strengthen accountability as a democratic value and a necessary component of national security (OSJI, 2013a, pages 8-9).

Scholarly commentary has also been consistent with this normative analysis. Roberts (2004: 683) argues that excessive state secrecy hinders the ability of citizens to govern themselves democratically by restricting their ability to debate issues of national importance. Similarly, Pozen (2009: 2327) describes

how so-called "deep secrecy" threatens constitutional checks and balances. The Tshwane Principles address these relative criticisms by redefining the relationship between transparency and security as one in which transparency is a pre-condition to establishing the legitimacy of security itself.

Also importantly, the principles necessarily incorporate public interest reasoning in national security decisions. By stating that such interests—such as government embarrassment or perceived political disadvantage—cannot justify secrecy, the principles are consistent with the principles of human rights law against abuse of power laid out in the aforementioned jurisprudence from International Authorities (OSJI, 2013b, p. 7). This characteristic of the principles, therefore, complements the principles of anti-corruption and rule of law previously discussed in this dissertation.

In summary, the Tshwane Principles act as a normative bridge connecting the broad guarantees of human rights to the specific realities associated with how governments provide security to their citizens. Although they are formally non-binding, the principles carry persuasive authority when used as guidance in interpreting laws and developing legislative schemes, and as a benchmark for assessing how states have established their own regimes for secrecy.

7.3 Key Principles on Disclosure and Secrecy

The Tshwane Principles articulate a comprehensive disclosure-first architecture for national security information, grounded in international human rights law and democratic accountability. At their core lies a strong presumption in favor of disclosure, reflecting the understanding that access to information is an essential condition for democratic participation and oversight, even in matters implicating national security (Open Society Justice Initiative [OSJI], 2013b, Principles 1–3).

Principle 1 establishes that everyone has the right to seek, receive, use, and impart information held by or on behalf of public authorities, including information related to national security, subject only to limited and clearly defined exceptions (OSJI, 2013b, Principle 1(a)–(c)). This presumption reverses traditional secrecy regimes that treat security information as categorically exempt. Instead, secrecy must be exceptional, justified, and temporary.

Importantly, the Principles reject categorical exemptions for entire institutions. No public authority—including intelligence agencies, armed forces, police, or the executive—may be excluded wholesale from disclosure obligations (OSJI, 2013b, Principle 5). This reflects comparative jurisprudence and scholarship warning that institutional blanket exemptions enable abuse, over-classification, and the concealment of wrongdoing (Roberts, 2004, pp. 72–75; Banisar, 2011, pp. 9–12).

A central contribution of the Tshwane framework is the harm test. Information may be withheld only where disclosure would pose a real and identifiable risk of significant harm to a legitimate national security interest (OSJI, 2013b, Principle 3(b)(i)). Speculative, generalized, or hypothetical harms are insufficient.

Even where a credible risk of harm exists, authorities must conduct a public interest balancing test. Disclosure is required if the public interest outweighs the risk of harm (OSJI, 2013b, Principle 3(b)(ii)). Factors favoring disclosure include, inter alia, promoting open debate, enhancing accountability, revealing misuse of public funds, exposing corruption, and uncovering human rights violations (OSJI, 2013b, Principle 3(b); OSJI, 2013a, pp. 4–5).

Crucially, the Principles specify irrelevant considerations—such as embarrassment to the government, political disadvantage, or loss of public confidence—which may never justify secrecy (OSJI, 2013b, Principle 3(b)). This clarification

directly addresses long-standing critiques that secrecy laws are frequently misused to shield officials from scrutiny rather than to protect genuine security interests (Pozen, 2009, pp. 279–284).

Principle 10 enumerates categories of information subject to a high presumption, or overriding imperative, of disclosure, even in national security contexts. These include information concerning:

- serious violations of international human rights or humanitarian law,
- safeguards against torture and arbitrary detention,
- structures and powers of government,
- surveillance programs,
- decisions to use military force,
- and accountability for constitutional or statutory violations (OSJI, 2013b, Principle 10).

For certain categories—particularly gross human rights violations—withholding on national security grounds can never be justified (OSJI, 2013b, Principle 10A). This position aligns with international human rights jurisprudence and reinforces the right to truth as an integral component of accountability (La Rue, 2013, paras. 74–77).

The Tshwane Principles emphasize that secrecy decisions must be accompanied by procedural guarantees, including written reasons for refusal, access to independent review, and judicial oversight (OSJI, 2013b, Principles 4 and 6). Oversight bodies must have access to all relevant information, regardless of classification, to perform effective scrutiny. This procedural dimension transforms disclosure from a discretionary favor into an enforceable right.

7.4 National Security Exception under the Tshwane Framework

The Tshwane Principles don't dispute the validity of using national security to deny access to information. They do, however, work on defining and limiting the national security exception to be consistent and compatible with democratic norms through stringent criteria and procedures.

A "national security" definition should be strictly defined in legal terms, and also be defined closely to the limits of a democratic country (OSJI, 2013b, Principle 2(c)). The requirement for a defined scope of measurement will help remedy the ambiguity seen in the research conducted on security. Research has shown that broadly defined concepts of security can lead to abuse of power (Wolfers, 1952, p. 481-483; Roberts, 2004, p. 70-71).

Only public authorities with explicit duties of protecting national security may apply the exception. Additionally, it is the government that has the burden of proof (OSJI, 2013b, Principle 1(d) and 4(a)). The mere fact that a minister has made a claim of potential damage is not enough to warrant restriction of access to information (OSJI, 2013b, Principle 4(d)).

Restrictions on access due to national security must meet a three-part test. 1) the restriction must have a clearly defined legal basis; 2) the restriction must be necessary to a democratic society; and 3) the restriction must be proportionate to the legitimate objective that is being pursued (OSJI, 2013b, Principle 3(a)-(c)). This mirrors the internationally recognized requirements for legitimate restriction of rights outlined in Article 19(3) of ICCPR and counterpart jurisprudence from regional agreements.

To meet the above criteria, there must be proof that there will be a specific and substantial damage as a result of disclosing

information, and that no alternative means of limiting the information (i.e. redacting it or disclosing parts of it) exist (OSJI, 2013a, p. 5). To meet the proportionality criteria, while limiting access to information, the extent of that limit must be the minimum necessary and may not damage the essence of the right to receive the information (OSJI, 2013b, Principle 3(b)(iii)-(iv)).

Article 8 of the European Convention on Human Rights outlines the limitations on the right to receive information, and provides additional support to this principle by demonstrating that national security cannot be a "trump card," which can deny all rights of access to information, especially if fundamental rights are involved (p. 8-11).The requirement for there to be limits on duration is an important part of this principle. National security restricts access to information only for as long as there is a reasonable expectation that there will be damage to national security due to the resulting disclosure (OSJI, 2013b, Principle 9). Comparative studies show that states are encouraged to establish a process for regularly reviewing and declassifying information, counteracting the developments of "permanent secrecy" identified by Pozen (2009, p. 301-304).

By requiring that national security be used in accordance with the established principles of legality, necessity, proportionality, and oversight, the Tshwane Principles redefine security and promote transparency, rather than create an environment that is generally opposed to transparency (Roberts, 2004, p. 76-78). Therefore, the Tshwane Principles redefine national security to be a limited justification, subject to constitutional, human rights and rule of law obligations. In this manner, TPT provides a credible balance between the protection of valid interests of security and the avoidance of security being used as an excuse for not being accountable.

7.5 Protection of Whistleblowers

The Tshwane Principles make a unique and innovative contribution in that they systematically provide for whistleblower protections in the national security context. The majority of right-to-information and freedom-of-expression frameworks dealt with disclosures made by public authorities but had few protections for individuals who disclose wrongdoing by security and intelligence agencies. The Tshwane Principles directly address this gap by recognizing that whistleblowing should be regarded as a legitimate mechanism of democratic accountability, rather than a threat to national security.

The Tshwane Principles acknowledge that disclosure of information by public officials and contractors can be in the public interest when it exposes serious wrongdoing, such as violations of human rights, corruption, abuse of power, or illegal surveillance (Open Society Justice Initiative (OSJI), 2013b, Principle 37). Thus, they align protection of whistleblowers with the public interest override doctrine, and reject the notion that all disclosures made by public officials or contractors that have not been authorized by the public authority are illegitimate.

As supported by Buckland and Wills (2013), whistleblowers often represent the only effective means of exposing institutionalized violations of law and human rights in the national security sector, which is often characteristically secretive, has limited external oversight, and is subject to existing laws that provide little protection for whistleblowers (pp. 6-9). The chilling effect caused by fear of retaliation for disclosures made without legal protection (e.g. criminal prosecution, termination of employment, or harassment) also reduces levels of transparency and accountability.

The Tshwane Principles establish the criteria under which whistleblowers shall be protected from civil, criminal, or administrative sanctions as long as a whistleblower:1. Has a

reasonable belief that the information disclosed evidences wrongdoing,2. Acts in the public interest, and3. Discloses information in a manner that is proportional to the various internal or external mechanisms for disclosure that are available (OSJI, 2013b, Principle 40).Importantly, the Principles reject the requirement that whistleblowers make prior internal disclosures when those mechanisms are ineffective, have been previously compromised, or place the whistleblower at a potential risk of retaliation. This position is consistent with the comparative literature, which highlights that internal mechanisms for disclosure within intelligence agencies are frequently not independent (Buckland & Wills, 2013, pp.14-17).

The Tshwane Principles establish a critical distinction between disclosures that would genuinely jeopardize national security and those that would only cause embarrassment to an institution or political inconvenience (OSJI, 2013b, Principle 37). Disclosures that would only cause embarrassment to an institution or political inconvenience explicitly cannot serve as legitimate bases for imposing punishment. The significance of this distinction is particularly important given the longstanding practice of governments prosecuting whistleblowers under broadly worded secrecy and espionage laws.

The UN Special Rapporteur on Freedom of Opinion and Expression has endorsed this position, emphasizing that whistleblower protections are integral to protecting the right to truth and preventing injustices associated with serious violations of human rights (La Rue, 2013, paras. 76-79). By establishing whistleblower protections within the framework of national security governance, the Tshwane Principles provide for the strengthening of the human rights-security nexus, rather than subordination of one to the other.

7.6 Oversight, Accountability, and Remedies

The Tshwane Principles assert that having substantive disclosure rules means nothing without strong institutional oversight and a way to find remedies. They therefore place a great deal of importance on independent oversight, judicial review, and effective enforcement mechanisms as foundational elements of a legitimate secrecy regime.

Principle 6 states that all oversight, ombudsman, and appeals bodies—including courts and information commissions—should have access to all relevant information regardless of the classification level (OSJI, 2013b, Principle 6). This ensures that oversight bodies have access to classified materials when they conduct reviews, so the review process is real instead of imaginary, which has been a long-time operational weakness in many national systems.

A comparative analysis shows that if oversight institutions do not have equal access to the relevant information, it is functionally meaningless. According to Banisar (2011), empowered, independent review institutions that can review secrecy claims, rather than automatically defer to what the executive says is necessary to keep secret, are necessary for effective RTI regimes (pp. 15–18).The Tshwane Principles unambiguously state that it is the burden of public authorities who wish to use national security to withhold information from having to justify their decision by providing specific and substantial rationales, showing a real and identifiable risk of harm from disclosure. Amounts to saying that just providing a general rationale or ministerial certificate is not enough.

This meets long-standing democratic principles articulated by Roberts (2004)—that lack of external scrutiny on executive discretion in decisions involving keeping information secret undermines public confidence in the government's accountability to the people and the Constitution (pp. 73–76). Therefore,

providing reasoned decisions is an essential safeguard against arbitrariness, rather than just a procedural formality.

Having access to judicial review is a key to the Tshwane principles. Individuals who do not have access to information must be able to appeal the decision to an independent tribunal with the authority to order disclosure where appropriate (OSJI, 2013b, Principles 6 and 38). Individuals should have timely and effective access to a remedy such that they are not kept from exercising their right to access information through unreasonable delay.

The European Court of Human Rights (Council of Europe, 2013) reinforces the need for judicial review for national security matters. Courts should assess both the necessity and proportionality of the decision to withhold information when deciding whether the right to access the information was violated, not simply the procedural correctness of the decision to withhold (pp. 10–12).The Tshwane Principles have operationalized a central democratic theory concept: unchecked secrecy actually diminishes the strength of the state. As it relates to national security, accountability strengthens security by preventing misuse of state power, correcting the failure of unjust institutions, and preserving the democratic legitimacy of an institution (OSJI, 2013a, pp. 8–9).

With respect to oversight and remedies, the Tshwane Principles challenge the conventional separation of secrecy and accountability. The Tshwane Principles contend that accountability can enhance security by preventing abuse, correcting institutional failure, and maintaining democratic legitimacy (OSJI, 2013a, pp. 8–9).With respect to a principle of democratic theory—unchecked secrecy undermines the strength of the State—the Tshwane Principles posit that oversight and remedies will, therefore, be constitutive components of a lawful

and effective national security policy rather than an external constraint imposed on national security institutions.

7.7 Applicability to Developing States

The Tshwane Principles have a central purpose of being relevant to all places throughout the world, including areas with developing or transition societies. In many of these societies, their secrecy laws were originally created during colonial or authoritarian eras, and the protection against national security bodies is weak. Therefore, the authors have created the principles to be practical and easy to understand by providing guidance for how to implement them rather than purely as a means of providing abstract norms (Open Society Justice Initiative [OSJI], 2013a, pp. 1–2).

All developing countries experience multiple difficulties that impede their ability to access information in the context of national security. Some examples include: broad secrecy statutes, poor independence of the judiciary, poorly-funded investigatory agencies, and a political culture that sees secrecy as a sign of strength (Banisar, 2011, pp. 7–11). These circumstances create an incentive for too much classified material to be created without adequate opportunity for review by the courts as to whether the classification claims are truly appropriate. Weak administration traditions increase the extent to which the executive branch dominates the process of classifying information, making it easier for the executive to undermine the right to access information (Roberts, 2004, pp. 72–75).

The Tshwane Principles provide a response to many of these problems by requiring minimum safeguards to protect democratic institutions and safeguards regardless of institution capacity. For example, limiting the executive branch from using categorical exclusions (Principle 5) and limiting the ability of the executive branch to place restrictions on rights to access information to limits that are established by law (Principle 3(a)) are particularly important in those situations where informal processes and the discretion of

the executive branch are the basis for deciding whether to allow access to information (OSJI, 2013b).

For example, when a developing state is contemplating legal reform, the Tshwane Principles serve as a model for developing legislation. They establish principles for legally justifying access to information laws, secrecy laws, and protections for whistleblowers to include tests of legality, necessity, and proportionality (OSJI, 2013a, pp. 4–6). Most importantly, while the Principles promote incremental implementation of reforms, they permit the priority of basic reforms (e.g. clarifying definitions of national security and establishing independent review) prior to implementing further proactive disclosure of information about national security.

The UN Special Rapporteur on Freedom of Opinion and Expression has openly supported the universality of application of the Tshwane Principles to all states by providing that the development issues of the state do not justify the use of blanket secrecy rules or the suspension of fundamental human rights (La Rue, 2013, paras. 78–80). This view confirms both the universal right to access information and makes clear that there is no applicable principle for limiting human rights protections in developing countries.

The Principles also call for building the capacity of oversight institutions, including information commissions, parliamentary committees, and the judiciary, and understands that developing states may lack sufficient resources to have adequate oversight institutions yet mandate that oversight bodies shall have access to classified information in order to adequately perform their oversight responsibilities (OSJI, 2013b, Principle 6). Access to classified information in developing states will assist the governments in curtailing the power of their executive branch and assisting the public in developing trust in the governance of national security.

In conclusion, while the Tshwane Principles should not be seen as aspirational goals for democracies that are mature; rather, they are

tools for advancing developing states towards developing lawful, accountable, and rights-protecting national security systems.

7.8 Tshwane Principles as a Balancing Model

The Tshwane Principles comprise a connected method for reconciling a state's need to protect its national security while at the same time supporting the public right of access to information. The Principles establish a more structured, predictable approach to balance than ad hoc or discretionary methods, by embedding the principle of balance through specific standards, procedural safeguards and oversight checks.

At the center of the Tshwane balancing model is a multi-layered framework established upon the principles of legality, necessity, proportionality and the public interest in assessing whether an act has been properly evaluated (OSJI, 2013b, Principle 3). These established criteria transform from a political judgment to a legal question and subject to independent review. The requirement of identifying a real and identifiable risk of significant harm ensures that claims of security are based upon evidence rather than speculation.

The principles are consistent with human rights law and address the issues of secrecy discussed in many articles (Pozen, 2009) and (Roberts, 2004) relating to the consequences of a lack of enforceable standards to prevent the establishment of "deep secrecy" and lack of institutionalized checks to limit executive powers (pp. 76-78).

As such, the Tshwane Principles place the public interest override to a significant degree within the model of balance. By providing for disclosure in cases where the public interest will outweigh the potential for harm and identifying certain types of public interest override to disclosure such as serious human rights violations, the Principles establish that the public interest override will not diminish accountability (OSJI, 2013b, Principle 10).This characteristic locates the Tshwane framework within a global

constitutional rule-of-law system, where transparency is a means to prevent abuse of power. Banisar (2011) states that without public interest overrides in secrecy regimes, it will perpetuate impunity and will ultimately undermine democracy (pp. 18-20).

The model of balance is further enhanced through the provision of protections for whistleblowers, independent monitoring, and effective remedies. These elements support the operation of balance in practice and establish that balance is to be more than just articulated in principle. As shown in the work of the Council of Europe, access to remedy and judicial review is necessary to prevent national security issues from being used as "trump cards" to displace fundamental rights (Council of Europe, 2013, pp. 10-12).

The normative coherence and transferability of the Tshwane Principles as a model of balance make it effective across different jurisdictions of law. By synthesizing international law, comparative practice and democratic theory into a single framework, the principles can apply to different constitutional requirements without losing the fundamental protections established under the principles (OSJI, 2013a, pp. 8-9).

For these reasons, the Tshwane Principles provide the most comprehensive articulation of how states may legitimately balance transparency against secrecy. The principles provide a benchmark against which national countries, especially developing countries, can measure their national laws and practices to ensure compliance with human rights law and democratic governance.

SECTION 8: Right to Information in Bangladesh — Legal and Practical Analysis

8.1 Constitutional Basis of RTI in Bangladesh

Bangladesh's Constitution does not specifically state the "right to information" as a stand-alone right; however, numerous arguments have been made for a constitutional basis for RTI from a right to freedom of thought, conscience, and speech (as well as the right to freedom of the press). Specifically, Article 39 is used as the main constitutional basis for RTI reasoning as it guarantees freedom of speech and expression while providing a framework for when the freedom can legally be restricted. Murad and Hoque detail both the content and the restrictions outlined in Article 39, which, similar to how freedom of speech or expression is guaranteed in the Constitution, is provided with a number of "reasonable restrictions" can be placed on exercising a right to freedom of speech or expression for a number of justifiable interests such as state security, public order, decency or morality, and so forth (Murad & Hoque, 2011, p. 79).

The constitutional structure is particularly important to a balancing book, as Article 39 serves not only as an express freedom of expression source but also as a constitutional map of competing public policy objectives that are frequently cited to justify limited access to information, particularly national security and public policy objectives that work to reinforce each other. The same constitutional rationale has also been linked explicitly to how the RTI Act in Bangladesh is structured in relation to exemptions—according to Karim, as a matter of constitutional law, Article 39 represents a guarantee of freedom of expression and freedom of the press but allows for the reasonable restrictions based upon national security; the list of exemptions from the RTI Act (Article/Section 7 of the RTI Act) "conforms largely to" the restrictions provided in Article 39(2) of the Constitution (Karim, 2013, p. 5). In short, the constitutional

rationale that supports RTI in Bangladesh is best understood as being dual in nature; it promotes openness through expressive freedom while also providing the constitutional basis for statutory exemptions (i.e. national security, public order, etc.) that have been created later in time.

Another argument that has been made in Bangladeshi RTI scholarship regarding a constitutional basis is that the RTI Act's stated purposes and commitments set forth in the preamble of the Act embody the constitutional promise of accountable government. According to Nigar, the preamble of RTI Act includes a "constitutional commitment" (Nigar, 2013, p. 128), which establishes RTI as an implementable body of constitutional law to achieve good governance principles grounded in constitutional law, such as transparency, accountability, and citizen empowerment. In constitutional terms, this view portrays RTI as not only an extension of each individual's freedom of expression but also as a means for citizens to hold public authority accountable; thereby strengthening democratic governance and the rule of constitutional law.

Accordingly, Bangladesh's constitutional basis for RTI can be expressed in three connected propositions:

1. Derivative-right argument (Article 39): RTI is anchored in freedom of speech, expression, and press, because effective expression presupposes the ability to seek and receive information, not merely to speak (Murad & Hoque, 2011, p. 79).

2. Limitation-structure argument: the same constitutional clause supplies a principled structure for restrictions—especially security and public order—making constitutional balancing unavoidable from the outset (Murad & Hoque, 2011, p. 79).

3. Governance-commitment argument: the statutory RTI framework is presented as implementing constitutional commitments to accountability and transparent public administration (Nigar, 2013, p. 128).

8.2 Right to Information Act, 2009: Overview

Bangladesh's RTI regime emerged through a rapid legislative sequence: the draft RTI framework was finalized and signed as an ordinance in October 2008, with the expectation of later parliamentary ratification. Murad and Hoque describe how the draft was reviewed, finalized, and signed as an ordinance by the President in October 2008, and then pursued for enactment in the subsequent parliament (Murad & Hoque, 2011, p. 81).

Karim summarizes the formal design of the RTI Act as containing eight chapters and thirty-seven articles/sections (Karim, 2013, p. 5). This structural point is useful for book drafting because it signals a relatively comprehensive legislative scheme: definitions and scope, procedures for requesting information, proactive obligations, exemptions, remedies/appeals, and the institutional framework of the Information Commission.

From an objectives standpoint, Nigar frames RTI as a legal right enabling a citizen to seek government-held information and to pursue legal remedy upon failure to receive it (Nigar, 2013, p. 128). This is a functional definition that aligns well with Section 8's emphasis on practice: RTI is not only declaratory; it is designed to be actionable through formal procedures and remedies.

The ability to use the 2009 Act is one of its main purposes by having clear procedures to access information. According to Nigar, applicants can either request information in writing or electronically (i.e., via email); however, the responsible officer is obligated to respond within the designated timeframe (Nigar,

2013, p. 131). Nigar has provided a three-tiered timeframe for responding and providing information: 20 working days (for standard personal information requests), 30 working days (for public data), and 24 hours (for urgent information) (Nigar, 2013, p. 131). This method of classification is important from a legal theory perspective because it establishes a time-limited framework for access and thus operationalizes RTI as a legally enforceable obligation rather than merely an administrative action subject to unfettered discretion.

Nigar also states that information can be provided in different formats, including electronically via e-mail; as well as by hard copy (photocopy/printed version); or on CD; and that the amount charged for providing information should not exceed the actual cost of providing that information (Nigar 2013, p. 131). The actual cost principle is a practical barrier to fees that would otherwise prevent individuals from effectively utilizing RTI.

Effective RTI systems are enabled by institutional design as opposed to the purely legal and constitutional framework that defines rights under the RTI Act. The Act clearly imposes duties on authorities to provide access to information under RTI, including requiring an agency establish a unit responsible for providing access to information; develop an index to facilitate storage of information as requested by Nigar; publish and publicly disseminate information proactively; and provide annual reports to the public as set forth (Nigar 2013, p. 130). Thus, these institutional design characteristics importantly help define the implementation and maintenance problems created by institutions having limited capacity (i.e., record management; index management; and creating an institutional culture of proactive public information delivery).

Any analysis of the RTI Act must include its exemption system because in order to achieve the goals of the book, the exemption system will help to demonstrate that obtaining a

balance is necessary. According to Murad and Hoque, in order to deny release of information based on the exemption criteria, Murad and Hoque assert that the basis for the denial must satisfy three criteria: 1) the information must relate to one of the legitimate purposes for restricting disclosure as defined by law, 2) it would be harmful to the legitimate purpose of withholding the information to disclose the information, and 3) the restriction on the public's right to access the information must outweigh the public interest in having access to that information, as set out in the RTI Act (Murad & Hoque 2011, p. 84).

The exemption list established in the Act is predominantly consistent with the restriction framework set out in Article 39(2) of the Constitution; therefore, the legal and statutory basis of the exemption under the Act is logically consistent with the constitutional "reasonable restrictions" on documents or information. This enhances the legal basis for supporting a legal theory that RTI has been "constitutionalized" and, therefore, it complies with both the constitutional value of freedom and value of being able to impose constitutional limitations. In addition, Murad and Hoque caution that the application of an expansive exemption list could create future problems because authorities do not consistently meet their burden to provide clear and reasonable written justification as to why each respective request cannot be granted (Murad & Hoque 2011, p. 86).

The legal foundation for a rights-based framework requires a system for redress of rights violations under the Act. The RTI Act includes a system for individuals to pursue redress when their requests are denied or not fulfilled, providing application right to pursue redress for denial or non-fulfillment of RTI requests (Nigar, 2013, p. 131). This portion of the Act is essential for evaluating the effectiveness of the RTI Act in Bangladesh's earlier years, as the effectiveness is not only governed by the existence of legal rights, but also whether a refusal to grant RTI requests is subject to judicial review and whether individuals

seeking enforcement of their rights can obtain timely and effective outcomes.

8.3 Institutional Framework: Information Commission

One of the distinguishing characteristics of RTI in Bangladesh is its establishment of an independent Information Commission (IC) as the main entity for oversight, enforcement and facilitation under the Right to Information, 2009. In terms of both doctrines, the Commission lays out the duties we must follow in order to use RTI by turning abstract access rights into concrete duties that can be enforced through review by the IC. The Access to Information Act, 2009 provides the IC with a quasi-judicial role which means that the IC handles complaints, hears appeals, issues guidance, raises awareness and provides information—this model fits within the IC and other RTI bodies' institutional frameworks across GSI.

The Act creates a three-member Commission made up of one Chief Information Commissioner and two Information Commissioners, who are appointed through a clearly defined statutory appointment process. Scholars note that true independence, such as security of tenure, fixed terms and limited grounds for removal, are important in establishing RTI dispute resolution authority (Nigar, 2013, pp. 130). According to Murad and Hoque, access to complaints and appeals from refusals/non-responses are critical to transforming RTI from a declaratory right into an enforceable right (Murad & Hoque, 2011, pp. 82-83).

The IC has a relatively broad jurisdiction and can apply its authority to all "authorities" defined by the Act (i.e. publicly owned ministries, statutory bodies and other institutions). The IC's potential powers of function include: (i) ordering disclosure; (ii) issuing directions for correcting recordkeeping and proactively publishing information; and (iii) recommending discipline or monetary penalties for authorities that do not

comply, under applicable statutory limits. Nigar describes that the IC may require the authority to provide a justification for refusing to provide access to information, thus shifting the responsibility for justifying a refusal to the authority and creating a presumption of disclosure (Nigar, 2013, pp. 130-131). The presumption of disclosure creates institutional fit for balancing because it greatly limits the discretion of the authority when making its first instance determination.

Beyond reviewing complaints and appeals, the IC has a number of standard-setting and awareness-raising responsibilities, including issuing guidance and training designated officers in their obligation to provide access to information under the Act. Many of the early empirical studies reported that inadequate records management and indexing procedures prevented timely access to information; thus, the IC's responsibilities for directing authorities to create good information management practices was essential (Karim, 2013, pp. 9-10). These facilitating responsibilities of the IC are consistent with the overarching principle of international best practice: namely, that the effect of RTI is determined by both the capacity of the institutions providing access to information via RTI, and the legal entitlements established under the RTI Act.

Bangladeshi scholars have cautioned that in its first years, limited resources, the reluctance of public authorities to comply and an existing legacy of an administrative culture of secrecy restrained the effectiveness of the IC (Murad & Hoque, 2011, p. 86; Karim, 2013, p. 12). Nevertheless, the fact that there is the existence of an independent review body represented a significant change in the landscape of Bangladeshi agencies: refusals were no longer absolute and justification for reasons for providing access to information became increasingly fundamental to balancing proportionality.

8.4 Exemptions under the RTI Act

In terms of where RTI intersects with privacy and state security, the exemption regime is the main legal site, and thus is of great importance to a book based on balance. The Bangladesh RTI Act outlines the exemptions from RTI by way of section 7 of the Act, where certain categories of information can be withheld if its release is likely to cause harm to the interests that are protected.

The primary categories of exemptions as provided by Murad and Hoque, include: information whose disclosure will be against the interest of state security; sovereign, territorial or international integrity; relate to law enforcement or the effective governance of a state; relate to personal privacy; subject to secrecy obligations (Murad & Hoque, 2011, pp. 84-85). The scope of the above exemptions broadly mirrors the constitutional grounds for restrictions under article 39(2), which Karim comments on, as he states that the exempt list under this statute is largely similar to "reasonable restrictions" as enumerated under the Constitution (Karim, 2013, p. 5).

As stated by Murad and Hoque, exemptions are not absolute in nature. Authorities are required to do more than simply identify the fact that an item of information must be withheld based on the category in which it fits, they are required to consider and assess the following: will disclosing the required information cause significant harm to the interest that it is protecting and the degree of significance of that damage vis-a-vis the pubic interest in disclosure (Murad & Hoque, 2011, p. 84). The three-part reasoning or logic (legitimate aim of withholding, determination of the level of harm caused by disclosing the requested information, and balancing of the damage caused by disclosing vs disclosure to the public interest) is consistent with proportionality analysis and meets the international standards.

Privacy is a separate and distinct exemption head where disclosure would result in an unreasonable, unwarranted invasion of

personal privacy. Nigar has highlighted that the calibration of the exemption head of Personal Privacy needs to be done carefully to prevent routine refusal of access to information regarding public officials performing their official duties (Nigar, 2013, p. 129). The challenge for Bangladesh as discussed in earlier Bangladeshi literature is determining what constitutes legitimate privacy claims as compared to those claims made for strategic reasons to protect maladministration.

Exemptions for state security are amongst the most commonly relied upon and is one of the most contested exemption heads. Murad and Hoque caution that the vague wording of state security exemption, such as information "likely to prejudice the security of the State," creates the risk of over-classification unless they are given a narrow interpretation and reasoned justification (Murad & Hoque, 2011, p. 86). Karim's field research provides many examples of authorities providing a security based rationale for their denial of access to information; however, he provides no instance of the authorities articulating specific damage to the required interest and this high level of authority abuse demonstrates the need for the Information Commission (IC), to exercise a more robust oversight role (Karim, 2013 pp. 11-12).

The exemption system's compatibility with RTI is ultimately dependent on procedural safeguards being in place: provide written reasons for refusals; provide a time limit for responding; provide the right of appeal to IC. Nigar asserts that these safeguards create the requisites for review of the discretionary shield of the exemption system and enable the applicant to provide proof that the criteria to withhold the information legally exists (Nigar, 2013, pp. 130-131). This ability to review the application of the exemption system provides a baseline for balancing RTI with privacy and security interests, and will lay the foundation for comparative and evaluative analyses in the following sections.

8.5 RTI vs Official Secrets Act and Other Laws

One major structural tension within Bangladesh's transparency regime relates to the conflict between the coexistence of pre-existing secrecy-oriented legislation, such as the Official Secrets Act, 1923 (OSA), and the explosion of access-oriented statutes established in the RTI Act, 2009. The OSA, which criminalizes the unauthorized disclosure of a wide range of official information using broad, indeterminate language, provides public authorities with excessive discretion and a de facto preference for executive control over information. This stems from the historical use of colonial secrecy laws as a normative default tool of administrative control and executive privilege. Conversely, RTI is presumed to be made public unless there are legally defined exemptions (and those exemptions are reviewable).

Despite the RTI Act's explicit purpose of promoting public access, it does not formally repeal the OSA; consequently, officials are left uncertain about the hierarchy or applicability of each law. Karim's empirical study shows that public officials continue to rely heavily on the OSA as a tool of protection against disclosing information that would otherwise require disclosure under the RTI Act (Karim, 2013, 13). In these cases, the mere existence of the OSA creates a chilling effect on an official's decision to disclose information to applicants, particularly in sensitive sectors such as defense, law enforcement, and foreign affairs.

From a doctrinal perspective, Bangladeshi RTI scholars commonly endorse the principle of lex posterior and lex specialis (i.e., the later law prevails over earlier laws; the more specific law prevails over the more general law) to argue that RTI should prevail over inconsistent secrecy laws. Murad and Hoque (2011, 88) have argued that the OSA should be overridden to the extent it is inconsistent with the RTI Act, as the RTI Act is a specific statute that was enacted to give effect to the constitutional values of transparency and accountability.

However, the absence of an express clause that the RTI Act or the OSA will take precedence has weakened the interpretive support for the principle of lex posteriores and lex specialis. Nigar (2013, 129) explains that in practice, many designated officers prefer to adopt a "risk-adverse" interpretation of legislation, thus preferring to maintain confidentiality and avoid possible criminal liability under the older OSA. Consequently, this administrative conservatism undermines the RTI Act's transformative purpose, thereby forcing RTI applicants to pursue an appeal process through the Information Commission.

In addition to the OSA, the RTI Act also coexists with various sector-specific confidentiality statutes and regulations (e.g., service rules, evidence laws, administrative instructions). For example, Karim (2013, 11-12) reports that public officials frequently rely upon confidentiality clauses contained in their rules of practice without first engaging in a harm-based and public interest disclosure analysis required by the RTI Act.

The reliance on confidentiality clauses reflects a broader structural issue of fragmented legal harmonization. The RTI Act is frequently given less priority as the governing legal framework with respect to access records than it is with respect to older or parallel legal frameworks. This produces inconsistent RTI implementation across governmental institutions. Thus, whether an applicant receives access to the requested record will depend more upon the culture of the governing institution than the governing statute.

8.6 Social and Administrative Barriers

The effectiveness of the Right to Information (RTI) regime in Bangladesh has been limited not just through legal processes but through social, administrative and cultural barriers. These barriers explain why the formal legal entitlements created through the RTI will not necessarily translate into actual meaningful access in practice.

A recurring theme in the RTI literature from Bangladesh indicates that the legacy of secrecy in the administration remains imbued by the former colonial governance structure and has been reinforced by extensive years of centralized executive power.

Numerous public officials view the information within their purview as their property, which makes it difficult for them to make such information publicly accessible, including at times when the RTI process requires them to do so or provides formal, legal mandates, (Murad & Hoque, 2011, p. 86).This barrier is further compounded by personal accountability fears of officials. In other words, making a RTI request is perceived to be a threat, as opposed to simply exercising one's right as a citizen, particularly in contexts of corruption, procurement and discretionary decision making.

According to Nigar, public officials and citizens alike do not necessarily know about their rights and obligations concerning RTI requests, particularly in the first few years following the enactment of the RTI, both had limited knowledge of: necessary procedures; time limits; and appeals processes (Nigar, 2013, p. 130). Therefore, potential applicants do not always know what they are required to do to make a RTI request, and the designated officials lack appropriate training in record keeping, analysis of what is exempt and then how to provide a reasoned decision.

Karim's fieldwork has also documented the inadequate procedures for the administration of recordkeeping, indexing and digitization of records have limited the speed with which an official can respond, even when he or she wishes to provide RTI access (Karim, 2013, p. 10). Without systematic reform of how records are kept and managed, the procedural guarantees provided by the RTI Act cannot function effectively.

The existence of social hierarchies and uneven distribution of power have had a negative affect on the number of RTI requests that are made. Specific populations that are most affected by inequities in the distribution of power: rural citizens, women and those that are

economically disadvantaged, have a much greater level of difficulty in making requests, following-up on requests and participating in the appeal process. Even though the RTI Act is, prima facie, neutral in its application, it is accessed and used in practice, quite differently by these populations due to lower levels of literacy, less access to administrative buildings and less familiarity with the legal process (Nigar, 2013, p. 131).The gap between equality on its surface and what actually exists in terms of access to RTI constitutes the basis of concern with the distributive element of the RTI and reinforces the argument that legal reform requires that it occur alongside social empowerment and institutional support.

The enforcement of the RTI Act will always be inconsistent. While the RTI Act states that there are both criminal and civil sanctions for Officers that fail to comply; Karim has noted (number 1) that there are very few instances in which these officers were fined thereby further weakening the deterrence for performing RTI obligations and perpetuating the non-disclosure culture (Karim, 2013, p. 12). The lack of enforcement further undermines the credibility of the Information Commission and suggests that administrative inertia is tolerated.

8.7 RTI, Privacy, and Security in Practice

In the early operational years of Bangladesh's RTI regime, the most decisive "real-world" tension has not been abstract conflict between rights, but how officials interpret and deploy exemption language in day-to-day administration. Karim documents that secrecy-oriented laws and oaths historically functioned as barriers to access, and that the Official Secrets Act, 1923—particularly its secrecy and offence framing—was repeatedly treated as a convenient justification for non-disclosure (Karim, 2013, p. 13). This practice matters because it shifts RTI from being a *right* into being a *discretionary privilege*, especially when officials fear liability or institutional blame.

The practical pattern is reinforced by the exemption structure itself. Karim notes that Article 7's exemptions are positioned as largely aligned with the constitutional restriction clause under Article 39(2), which already frames free expression as subject to restrictions for security, foreign relations, public order, and related grounds (Karim, 2013, p. 16). In practice, this alignment often encourages decision-makers to treat "security" as a *broad umbrella* rather than a narrowly demonstrable harm-based exception.

Similarly, Nigar observes that Bangladesh's RTI Act restricts the right by exempting "twenty kinds of information," including categories tied to security, integrity/sovereignty, and foreign relations (Nigar, 2013, p. 7). Therefore, the practical conclusion is that 'security-related language' has become a standard form of/ or routine administrative language in Bangladesh for refusal of requests, regardless of whether the significant interest of the public in having access to, for example, how public resources will be allocated, how services will be delivered, or how requests for information related to corruption are valid. A common sentiment echoed throughout Bangladesh's RTI literature is that the exemptions provided under RTI are too broad and open to misuse unless accompanied by sufficient interpretative guidance and a strong culture of providing reasons. According to Murad & Hoque, the exemption categories seem to be comprised of categories related to national security, sensitive economic information, personal privacy and sub judice; however, unless there are clear guidelines established for the application of the exemptions, the excessive scope of the exemption categories will allow for abuse because of their excessive vagueness (Murad & Hoque 2011: 14).

There are areas of privacy that are particularly controversial, such as providing protection for the dignity and autonomy of individuals. Although privacy can be an appropriate means of protecting the dignity and autonomy of individuals, it can also be

used as a strategic screen to cover up information that should be disclosed to the public (i.e. information dealing with public functions or expenditures, integrity in the operation of government, etc.). Nigar argues that the limitations in the statute (particularly in respect of the exempt list) adversely affect the implementation of the Act and create "interpretive opportunities" for limiting the application of the Act. The key "point of practice" is the extent to which refusals are subject to meaningful review. Murad and Hoque describe the initial level of decision, subsequently the appeal to an agency of the government, and potentially the court level; they summarize the appeal process and express that they expect the review on the refusal to be independent. However, merely having "formal appeal rights" will not guarantee compliance by applicants where there is a distance between themselves and the agency, cost, lack of knowledge of the process or long delays.

Karim indicated that the implementation at the grassroots was subject to obstruction where designated officers were uncooperative and there were ambiguities in the statute, particularly in respect of the appellate body, which created operational difficulties for the Information Commission in making decisions. In practice, this means that the Commission's administrative mandate would not be implemented as effective and reliable remedies will only be available if the broader administrative environment provides support for the Act.

The success of the implementation of RTI is dependent on the quality of record-keeping systems. In his report, Karim indicated that many offices do not maintain adequate systems for preserving/managing and publishing records, records are often kept in a "haphazard" manner, and significant time is needed to locate records requested by applicants. These conditions create delays and dissuade applicants from using the RTI law. Karim also pointed out that there have been some failures by the agencies to disclose records on a proactive basis; for example,

they often fail to submit their annual reports in a timely manner, they do not update their website, and they have not implemented current practices for preserving records. All of these issues serve to increase the pressure on designated officers and serve to provide increased opportunities for harassment or delay (Karim, 2013, p. 30).

Complementing this view, Hoq stated that laws cannot by themselves guarantee democratic rights and that the implementation of laws requires a supportive information ecosystem and avenues to meet information needs, including library and information centres. Consequently, this indicates that evaluating the RTI regime in Bangladesh cannot only be done legally, but must also include evaluation of the level of the information infrastructure, professional competency, and incentives provided.

8.8 Critical Evaluation of the Bangladeshi Framework

The RTI Act in Bangladesh is changing how the country is run by providing citizens with access to information on a formal basis instead of behind closed doors or just for officials. Nigar refers to the fact that RTI has been recognized as a legal right as an "epoch-making step," as it demonstrates how the Rest is now evolving into a governance tool based upon rights (Nigar, 2013, p.12). The creation of an Information Commission and specifying authorities' roles (units, retention, publication) indicates that the structure of the Act will not just reactively respond to requests. It will also proactively create transparency for citizens (Nigar, 2013, p.7).

The coexistence of broad exemptions with a durable secrecy tradition is the greatest structural-legal shortcoming. Murad and Hoque's comment about the broad exemption clause and how it could be abused illustrates one of the most important legal risks: as the exemption clause expands so does the narrowing of the right to access (Murad & Hoque, 2011, p.14). Karim's history of

the institution supports this conclusion because historically, the secrecy-based laws and policies have been an obstacle to the flow of information to the public, and officials have sought refuge from their obligations to contribute to the flow of information by advancing the Official Secrets Act (Karim, 2013, p.13).

A sufficiently comprehensive evaluation can be made: While in its intent Bangladesh's RTI framework is progressive, it is partially obstructed by an unaddressed conflict between secrecy-based institutions and the inherited culture of bureaucratic administrative practices. Creating formal agreement between the two will allow officials to be more confident in their decision to comply with RTI requests, and then be clear that the RTI framework governs the making of disclosure decisions regarding the disclosure of those records received in the course of their daily administrative work.

Nigar identifies many practical problems hindering the enforcement of the RTI Act, including but not limited to deadlines, the location of the Information Commission, lack of proactive and proactive incentives for disclosure, and ambiguity in the court process for litigation under the Act, all of which inhibit ordinary requesters from having access to RTI (Nigar, 2013, p.12). Karim extends these concerns into the administrative review process, among others, by stating that the lack of an "expiration" policy of publication, the lack of opportunities to develop electronic capabilities, insufficient record retention efforts, limited logistical support, and the broader socio-economic factors of literacy and awareness limit both the "demand side" and "supply side" of RTI (given that both the demand and supply consist of the ability to produce records that give a requester access to RTI) (Karim, 2013, pp.30-34).

One more evaluative conclusion can be drawn: even a RTI law that is drafted properly cannot serve its intended role in the constitutional-democratic framework of government if the access

infrastructure (such as records, training of staff, information and communications technologies (ICT), and STL) are lacking or underdeveloped. A significant part of Hoq's argument for an information ecosystem is that the implementation of RTI requires capacity-building both within and outside of the entity or profession mandated with enforcing compliance with the RTI Act (Hoq, 2013, p.2).

From a balancing doctrine viewpoint, Bangladesh's RTI framework needs stronger interpretive discipline in three areas:

1. A harm-based security test (security should not be a label; it should require a reasoned showing of likely harm).

2. A clearer privacy standard distinguishing personal sensitive data from information about public functions, public expenditure, and official accountability.

3. A robust public-interest override culture, so that where disclosure serves accountability and anti-corruption aims, exemptions do not become blanket shields.

Murad and Hoque underline the necessity of independent review and structured appeals (Murad & Hoque, 2011, p. 14), but the practical record shows that without consistent reasoning practices and enforceable compliance incentives, exemptions can dominate outcomes.

Bangladesh has taken a decisive legislative step toward transparency, but the regime's effectiveness remains constrained by: (i) unreconciled secrecy laws, (ii) broad and misuse-prone exemptions, (iii) implementation capacity deficits, and (iv) uneven accessibility for citizens. The critical direction for reform is therefore not only "more RTI," but better balancing architecture—legal clarity, harmonization, institutional strengthening, and a compliance culture grounded in reasoned decisions and meaningful review.

SECTION 9: COMPARATIVE AND BALANCING ANALYSIS

9.1 Comparative Overview: Developed vs Developing States

The diverging growth of the Right to Information (RTI) in which there exists significant difference between advanced nations and developing nations is less of a normative commitment and more about how well they can implement, define and balance the requirements of transparency with privacy and national security. The realization that RTI laws have begun to emerge globally is sound, but the manner in which they are being designed and implemented does reflect the differing governance models, administrative cultures and socio-political limitations of each nation's government.

According to Ackerman & Sandoval-Ballesteros, RTI laws have proliferated significantly across the world with what the authors call a "global explosion," whereby access to information legislation expanded rapidly in both developed and developing democracies by the mid-2000s, (Ackerman & Sandoval-Ballesteros, 2006, pp. 85-88). However, the authors also found in their comparison that even though RTI legislation was being transplanted from advanced to developing nations, the legislation produced and operations of that legislation did not result in functionally similar results; in developed nations, RTI legislation was developed as an enhancement to existing accountability mechanisms and in developing nations, RTI legislation is viewed as a transformational reform to address the issues of corruption, non-transparency and weak institutions (Ackerman & Sandoval-Ballesteros, 2006, p. 99).

In developed nations like the UK, Canada and Australia, RTI legislation exists within the context of established constitutional frameworks that feature independent judiciary systems, professional public service and sound record keeping. In

contrast, RTI legislation in developing nations exists within administrative frameworks that feature a high degree of discretionary authority on the part of the bureaucracy, have inadequate documentation systems and were the byproduct of colonial administrative systems that had deep-rooted secrecy norms.

As the examples of empirical comparisons find, openness does not necessarily lead to an increase in trust from the public towards the government, especially in situations where institutions are not responsive. Worthy's examination of the UK Freedom of Information Act of 2000 indicated that although the amount of information that was disclosed increased exponentially, public trust in government did not also increase (Worthy, 2010, pp. 561-563). This finding is important in a comparative analysis of RTI's because it reflects that the determination of RTI's effectiveness goes beyond merely providing access to information; the manner in which that information is provided, explained and utilized also must be included in determining RTI's effectiveness.

In developing countries, this problem is more serious and pressing because of the burden created by overly broad exemptions, insufficiently independent oversight bodies, and limited resources for enforcement of RTI laws. Therefore, RTI laws do not fulfill their potential to transform societies (Ackerman & Sandoval-Ballesteros, 2006, pp. 111-113). As was discussed earlier in Sections 5 and 6, the broad use of national security and personal privacy exemptions are used far too often; they are treated as a "go to" means of refusal to provide access under RTI laws rather than narrowly defined exceptions.

In developed countries, comparative jurisprudence indicates that harm tests and proportionality analysis are frequently being utilized for balancing rights to RTI with rights to privacy and national security. According to Peled and Rabin, when RTI is

constitutionally recognized, access to information is commonly understood to be a derivative of the right of freedom of expression and, therefore, the state must provide compelling justifications for imposing restrictions on access and those justifications must be proportionately implementable (Peled & Rabin, 2011, pp. 370-374).

However, developing countries such as Bangladesh continue to utilize categorical exemptions as opposed to balancing freedom of access to information on a case-by-case basis. The continued use of categorical exemptions makes it unlikely that the growing trend to misuse RTI will be resolved. The research of Caidi and Ross supports the notion that transparency frameworks are structurally weakened when national security is defined very broadly and in a highly abstract way (Caidi & Ross, 2005, pp. 670-672).

9.2 Bangladesh in Comparative Perspective

The RTI legal framework requires comparative evaluation from the perspectives of (1) developed RTI jurisdictions (2) developing RTI systems that enacted access to information laws in the late 2000s. From a formal legal perspective, Bangladesh's Right To Information Act (RTI), 2009 conforms closely to international RTI instead. However, the Act makes access to information a statutory right; establishes an independent Information Commission; imposes duties on public authorities to disclose information to the public. Murad and Hoque (2011) have indicated that the Act embodies critical principles set out in international documents and below on international RTI best practices including Johannesburg Principles (Murad & Hoque, pp 74 – 76, 2011). In addition to conformity, Bangladesh's RTI legal framework, when compared to developing democracies that also enacted RTI laws around the same period (India 2005 & Indonesia 2008) has the same emphasis on citizen empowerment and administrative accountability.

Though the RTI legal framework conforms normatively, it diverges sharply in institutional preparedness and coherence when compared to developed RTI jurisdictions; while RTI laws in developed jurisdictions supersede any previously existing secrecy laws or practices, the Official Secrets Act of 1923 remains as another statute alongside the RTI including a lack of clarification of their coexistence resulting in an ambiguity of interpretation of the two Statutes and fostering bureaucratic risk aversion (Karim, pp 13 - 14, 2013). With respect to developing states, Ackerman and Sandoval-Ballesteros (2006) indicate that typically developing states fail to integrate RTI laws with the legal framework resulting in fragmented disclosure regimes (Ackerman & Sandoval-Ballesteros, pp 114, 2006). Bangladesh reflects this fragmentation, particularly when officials continue to operate under prior secrecy laws and instead of disclosure principles as set out in RTI laws.

According to Cuillier & Piotrowski's (2006) multinational research, they conclude that access to government records is linked to Executive capacity to seek information and government responsiveness (Cuillier & Piotrowski, pp., 444 - 446, 2009). In Bangladesh and shown in the sections cited below, limitations such as poor record management, digitization efforts and limited public education have resulted in an otherwise limited practical value for RTI due to the extent of limitations.

Hoq also places Bangladesh within a broader context for developing states indicating that for successful implementation of RTI laws, legal guarantees alone are insufficient, but there must also exist systems of professional records management and training of intermediaries who will facilitate the substantial use of RTI (Hoq, p 45, 2013). In ended terms, Bangladesh falls closer to transitional RTI regimes as compared to full developing transparency models. In comparative terms, Bangladesh’s RTI framework can be described as progressive in intent but limited in execution against other developing systems. Although

developed countries have begun analyzing the standards of balance using legal principles and reasonable basis analysis, Bangladesh is heavily dependent on the use of exclusionary provisions to deny citizens access to records through the decision of the public authorities. The gap in comparison with other developed countries stressed the issue of producing clearer guidelines for defining balance and oversight and legislative clarity.

9.3 Lessons from International Best Practices

Comparative experience indicates that effective right to information (RTI) regimes are not dependent on just having access legislation but rather through having coherent legal design, independent institutions to oversee actions taken by governments under these laws, and other mechanisms used to balance the competing interests or rights of transparency, privacy, and state security. International best practices provide examples of what types of information should be disclosed; how disclosure decisions are structured; and how disclosure decisions are reviewed.

One of the most common themes relating to mature RTI regimes is the presumption of disclosure. Ackerman and Sandoval-Ballesteros demonstrate that successful RTI regimes inverts the secrecy model and places the burden of justification on the government to prove that the information being withheld cannot be disclosed (Ackerman & Sandoval-Ballesteros, 2006, pp. 92–95). In jurisdictions such as Canada, United Kingdom and many European states, exemptions are treated as exceptions to a general presumption of openness rather than being treated as parallel regimes of secrecy.

Comparative studies have shown that exemptions relating to national security or confidentiality that are framed broadly or categorically will result in an expansion of the exemption in practice. Caidi & Ross also note that national security

exemptions are often abused when defined imprecisely, and they do not have harm-based thresholds (Caidi & Ross, 2005, pp. 670–672). Consequently, exemptions must be interpreted narrowly and applied only when the existence of demonstrable harm to a legitimate interest is present.

A second core principle of effective RTI regimes is the presence of independent oversight bodies with sufficient authority to conduct thorough reviews of refusals. Comparative research indicates the importance of information commissioners or similar independent bodies to turn RTI into an enforceable right rather than simply a formal right. In jurisdictions where the information commissioners are not separate from the executive and do not have enforcement capabilities, access to information legislation will continue to be symbolic (Ackerman & Sandoval-Ballesteros, 2006, 108 – 110).

Worthy's analysis of UK experience confirms this conclusion in that while the number of disclosed records since the implementation of the FOIA 2000 has increased, the continued legitimacy of the framework depends upon oversight institutions and courts being able to review claims made by the executive concerning exceptions to access (Worthy, 2010, 568 – 570). Best practices also highlight independence from the executive; transparent reasoning; and the availability of judicial review as essential to effective oversight.

Another important lesson learned from international experience is the need for a public interest override to exemptions to access to information legislation that are related to privacy or national security. Comparative RTI regimes recognize that even if an exemption meets the technical requirements under law, the information still must be disclosed if the public interest in disclosure outweighs the harm that may result from disclosure.

Banisar's examination of several RTI regimes is particularly instructive in that public interest overrides serve as a balancing

point against exemptions being applied mechanically to information; especially when corruption, abuse of power, or threats to democratic accountability exist (Banisar, 2011, 15-17). Without public interest overrides, RTI regimes can become rule-bound, and therefore they will not consider the totality of the contextual elements of each disclosure request; consequently they undermine the democratic legitimacy of RTI.

International best practices also emphasize the fact that the effective operation of RTI is contingent on sufficient organizational capacity, including trained staff, effective record management systems, and proactive disclosure policies. Cuillier & Piotrowski found a strong correlation between public support for access to information and the usability/accessible information systems (Cuillier & Piotrowski, 2009, 444 – 446). Developed countries generally introduce complementary reforms, including improvements to archives, digitizing records, and providing training for staff at the same time as they introduce RTI legislation. In contrast, developing countries typically lag behind developed countries in all of these areas.

9.4 Proposed Balancing Criteria

A set of normative balancing criteria can be proposed to establish principled, consistent methods of reconciling RTI with privacy and national security, using the lessons learned from comparative analyses and the doctrinal analyses discussed in previous sections of this book.

Access restrictions on information should be defined by law, and should be articulated to be sufficiently clear in their wording and language so that both requesters and administrators can understand their respective roles. According to Peled and Rabin, a constitutionalized RTI framework mandates that restrictions or limitations are foreseeable and factually stated so that there is a clear distinction between the exercise of discretion and the potential abuse of discretion (Peled & Rabin, 2011, pp. 371–373).

Using vague or open-ended exemptions, especially for national security, violates this requirement and is inconsistent with democratic principles.

Restrictions on access to information must pursue a legitimate objective such as and include such things as protection of state security, and/or individual privacy, and must be based on demonstrable risks to take such action. Caidi and Ross argued that claims of security should have evidentiary basis; otherwise, they will not be a legal justification, but instead serve as a political slogan (2005, pp. 671–672). Best practices therefore, require decision makers to clearly articulate, based on evidence, how the disclosure of information would lead to a particular harm, and not solely to make general claims about a class of information being 'sensitive'.

Two of the principles that are central to balancing methodologies are necessity and proportionality, which were previously discussed in Sections 5 and 6 of this book. Worthy's comparative study identified that jurisdictions where no proportionality analysis is completed typically over-withhold information, and therefore, the framework fails to build trust and accountability (Worthy, 2010, p. 570). Proportionality also requires that if some harm exists from the disclosure of information, the evaluating authority must consider alternative forms of access to the information (i.e. partial disclosure; redaction; or delayed disclosure).

A key aspect of any system of balancing will be the existence of a public interest override (allowing disclosure of information where there exists a location of transparency that is essential to the functionality of democracy). Banisar notes that public interest considerations become particularly important when reviewing potential disclosure in cases concerning corruption, abuse of public funds, or breakdowns in systemic governance (Banisar, 2011, pp. 16-18). The existence of this criterion contributes to the

functionality of the RTI system as an instrument of administrative law; however, it also attributes to the RTI process productive methodology for purposes of accountability and transparency.

Lastly, any determination made by the evaluating body in balancing of competing privacy and disclosure interests must be subject to independent review and reasoned written rationale. Ackerman and Sandoval-Ballesteros highlight the need for independent oversight and review in an RTI system so that an oversight body can scrutinize the merits and reasoning supporting a decision to deny access (2006, pp. 109–111). Balancing interests through a lack of transparency and review will ultimately result in unchecked administrative discretion in the determination to disclose or deny access to information.

9.5 Role of Clear Definitions and Legislative Precision

A central lesson emerging from comparative RTI regimes is that the quality of legal drafting—particularly the clarity of definitions and precision of exemptions—largely determines whether the right to information operates as a genuine democratic entitlement or as a formal promise undermined by administrative discretion. Legislative ambiguity, especially in relation to "national security," "public order," and "privacy," has repeatedly been identified as a structural weakness in access-to-information frameworks.

Comparative studies demonstrate that vague or open-ended statutory language invites over-classification and routine refusal of information requests. Ackerman and Sandoval-Ballesteros observe that in many developing states, RTI laws adopt broad exemption clauses without defining key terms, thereby enabling secrecy to persist under the guise of legality (2006, pp. 103–105). By contrast, jurisdictions with more mature transparency cultures define exemptions narrowly and exhaustively, reducing the scope for discretionary expansion.

The problem is particularly acute in relation to national security. As discussed above, the absence of a precise definition allows security to function as an elastic concept rather than a legal standard. Caidi and Ross argue that information regimes which fail to articulate concrete criteria for security-based restrictions effectively transform security into a default justification for non-disclosure (2005, pp. 670–671). Legislative precision therefore operates as a first-order check on secrecy.

Clear definitions are equally critical in balancing RTI with privacy. Comparative practice shows that privacy exemptions work best when they distinguish between personal data with no public relevance and information that, although personal, relates to public functions or public expenditure. Banisar notes that laws lacking such distinctions often permit authorities to invoke privacy to shield corruption or maladministration (2011, pp. 12–14).

Peled and Rabin's constitutional analysis underscores that precision in privacy clauses is essential to preserving the constitutional status of RTI itself. Where privacy is defined expansively without reference to public interest considerations, the right to information risks being subordinated rather than balanced (Peled & Rabin, 2011, pp. 376–378).

From a rule-of-law perspective, legislative precision enhances foreseeability and legal certainty. Requesters must be able to anticipate the grounds on which information may lawfully be withheld, while officials must be guided by clear standards rather than discretionary instincts. Worthy's comparative assessment of the UK FOI regime highlights that clearer statutory language improves consistency in decision-making and strengthens public confidence in the system (2010, pp. 567–568).

Accordingly, international best practice supports the conclusion that clear definitions, narrowly tailored exemptions, and explicit harm thresholds are indispensable elements of any

credible balancing framework between RTI, privacy, and state security.

9.6 Strengthening Oversight and Accountability

Although the law defines the parameters of RTI, the ability for the law to be fully appreciated will depend on the institution's ability to have procedures in place to uphold their obligations to disclose, as well as to review their refusals to disclose. Comparative analysis demonstrates that laws can be quite precise without independent institutions that can enforce disclosure obligations and review refusals.

The most obvious commonality among successful RTI systems is the presence of an independent information commissioner or oversight authority, with the authority to review administrative decisions. Ackerman and Sandoval-Ballesteros further provide that these bodies function as institutional checks on the surrounding environment from being overly influenced by the executive branch in matters of secrecy such as those, which may be otherwise politically volatile (2006, pp. 108-111). If the oversight body does not have independence, resources, or enforcement authority, the RTI is often not fully utilized.

Additionally, consistent with Worthy's findings, the role of the oversight body provides a dual function of resolving disputes as well as ultimately establishing the norms, and in time will influence the administrative culture towards openness (2010, p. 570). This cultural influence of oversight is particularly relevant in transitioning political systems that have previously had a legacy of governance based on secrecy.

A second pillar of accountability is judicial oversight of the executive. A review of the case law of various jurisdictions indicates that the courts provide a critical role in determining what the standard will be when balancing the competing interests, especially when the legislature is either silent or

ambiguous concerning those balancing standards. As noted by Peled and Rabin, the constitutionalizing of the RTI creates a situation whereby disputes about access become rights-based rather than discretionary decisions (2011, pp. 385-387).

Accountability is also dependent on the authorities providing reason for their decisions. Authorities must be required to provide a written explanation of the rationale for why the requested information would be harmful and the public benefit will outweigh the harm to the requestor. Banisar also states that the existence of a written justification significantly reduces arbitrary refusals, and therefore, increases the likelihood of a meaningful appeal (2011, pp. 18-19).

Oversight is particularly important when national security has been claimed as a basis for refusing access to information. As can be deduced from the comparative research, if investigations do not occur concerning the validity of national security claims, the claims generally expand to cover information that is no longer of a national security nature. Caidi and Ross warn that without independent oversight of national security claims, all national security claims will be self-reinforcing and will effectively disappear from accountability (2005, pp. 672-673). Therefore, best practices [in systematically strengthening RTI systems] must ensure that the oversight bodies and the courts)[a comment on independent governments or other nations having oversight functions, not related to RTI, is warranted here, potentially an indicator of reverse colonialism (that is, colonization of the people through government programs)] have unrestricted access to classified/sensitive information necessary to determine whether or not the claim is valid.

Finally, strengthening the oversight functions of the RTI and the courts not only increases the compliance of access requests but it also enhances the legitimacy of an open democracy. According to Cuillier & Piotrowski, if there is an effective and

impartial oversight body, the public will be more likely to support access rights (2009, pp. 444-446). Therefore, if RTI fails to demonstrate its accountability, transparency is at risk for generating skepticism, conversely, if there is no transparency in the RTI system, accountability will ultimately be lost in secrecy. Thus, sustainable RTI systems must rely on both the accountability and the transparency of both.

SECTION 10: CONCLUSION AND RECOMMENDATIONS

The objective of this book was to explore the Right to Information (RTI) through the prism of its inherent conflict with respect to state security and the right to privacy, with a particular focus on international standards of law and the national context of Bangladesh. The significant finding of this research study is that RTI, privacy, and state security are not fundamentally contradictory freedoms/interests, but rather interrelated legal principles that must be carefully and ethically balanced in accordance with democratic rule of law.

The research indicates that the right to information has transitioned from being derived from the inherent right to freedom of expression into being an independent, stand-alone human right, situated firmly within the international human rights legal framework and theory of democratic governance. RTI provides the foundation upon which transparency, accountability, and public participation are based, and implements practical facilitators for many other civil/political, economic, and social rights. However, this study finds that RTI is not an absolute right, and must be measured against legitimate constraints borne out of respect for individuals' privacy, and the protection of national security.

A fundamental research finding is that conflicts between RTI and privacy arise more as a function of conceptual misinterpretations and broad legal definitions, than as a function of actual incompatibility. When privacy is interpreted appropriately as a means of protecting human dignity and autonomy, it serves to promote RTI by limiting arbitrary or abusive disclosures. The research further demonstrates that state security, when defined narrowly and subject to legal controls, can coexist with transparency without threatening the existence of a democratic form of government.

The comparative analysis of RTI across jurisdictions reveals a constant and consistent pattern: where there are vague exemptions, there is insufficient oversight, and there is no proportionality test, secrecy generally prevails. On the other hand, jurisdictions that contain unambiguous legal definitions, provide for overrides based on public interest, have independent review authorities, and include judicial review, are more successful in balancing the RTI against legitimate limitations.

An in-depth look at the Bangladeshi experience provides insight into this more general dynamic. The Right to Information Act of 2009 reflects a strong commitment to transparency; however, the implementation of ANI, as currently written, is severely hampered by lack of resolution of conflicting provisions of law; resistance from public authorities; inadequate institutional capacity; and insufficient public understanding of the law. This analysis indicates that the problem is structural as opposed to incidental, and is closely related to the fact that a definitive balance of competing principles has not been fully developed in practice.

Finally, another finding of this analysis is the importance of the Tshwane Principles as a normative and operational framework for balancing access to information with issues related to national security. Specifically, the Principles set forth harm-based; necessity; and proportionality standards that are consistent with democratic constitutional values, and offer a workable template to any state that wishes to move away from blanket secrecy as a policy.

By reviewing the results of my research, I can respond to the original questions posed as part of my study.

First, RTI as a legally enforceable right has been recognized by international human rights law and democratic theory. The study confirms that RTI fulfills a major role - underpins accountability, participation, and rule of law - and should be

viewed as a legally enforceable right that may not just be mere administrative convenience. RTI being included in national, state, and international laws demonstrates its important function in modern day governance.

Second, the study concludes that there is no inherent conflict between security issues and RTI rights; conflicts arise from poorly drafted laws, broad interpretations of security, and the misuse of privacy claims - not from the nature of these two competing rights. Defining security in a narrow fashion and restricting its application through the use of necessity and proportionality principles renders security and the right to privacy legitimate limitations instead of tools of obstruction.

Third, in studying how various types of legal systems address the competing rights of RTI and privacy/security interests, it was found that different legal systems use different balancing mechanisms. Developed legal systems generally utilize contextual/harm-based analysis and possess strong oversight in balancing the competing interests. Many developing legal systems, including Bangladesh, continue to utilize broad exemptions, administrative discretion, and historical customs. This difference in the method used by developed and developing countries to balance competitive interests offers a better explanation for differing outcomes of implementation than do different formal commitments to RTI.

Fourth, as for Bangladesh, the research confirms that although there is a reasonably solid framework under law supporting RTI in Bangladesh, implementation is sporadic and weak. The presence of conflicting secrecy laws, limited authority of the oversight mechanisms, and social/cultural barriers are the greatest obstacles to the realization of RTI in Bangladesh. An additional weakness is the failure of Bangladesh to recognize and apply a comprehensive, consistent definition for the competing rights of RTI and security/privacy.

Finally, when considering whether it is possible to develop an effective model for balancing RTI and state security/privacy rights, the study concludes that the Tshwane Principles provide the clearest, most coherent, and most democratic framework available for this purpose. The Tshwane Principles articulate in simple, understandable terms how to determine the extent to which RTI should be disclosed, what security-based restrictions may be applied to RTI access, how to provide whistleblower protection and how to adequately oversee the implementation of RTI by public administrators. This framework can be effectively applied by both developed and developing countries.

The responses detailed above support the central premise of this book - the challenge is not whether RTI can exist together with state security/privacy rights; rather, the challenge is whether legal systems have the ability or willingness to apply principled, transparent, and accountable mechanisms to balance the rights of RTI with privacy and state security.

The findings of this research reveal an ongoing series of legal and institutional barriers that hinder the effective exercise of the right to information and distort its relationship to privacy and national security. These barriers are not limited to a singular jurisdiction; instead, they appear repeatedly throughout many legal systems and, in particular, are easily observed in developing nations. At the legal level, one major gap is the lack of precise definitions in statutory law. Terms such as ‘national security’ and ‘public interest,’ as well as the more general term ‘personal information,’ are often framed too broadly, or otherwise in an indeterminate way, permitting a great deal of discretion by public authorities. This results in diminishing legal certainty, undermining foreseeability and providing for the routine application of exceptions without a sufficient basis of justification. In particular, the interaction between RTI laws and previous secrecy laws creates normative ambiguities, often in

favor of secrecy over disclosure, because of the lack of any clear hierarchy or rules for their reconciliation.

A different legal gap related to this is the failure to properly incorporate balancing standards into domestic RTI laws. While international standards call for the application of necessity and proportionality principles as well as a basis of harm, these principles are not always present in national legislation or even in the practice of administrative entities. Consequently, decision-making often depends on categorical exclusions rather than evaluation of the particular context in which a decision is made, thereby reducing the flexibility required to deal with complicated cases with competing rights.

As an institutional constraint, the lack of adequate oversight systems has also been identified as a significant limiting factor. Information commissions and other oversight bodies do not have sufficient independence, resources or enforcement authority to effectively challenge an additional level of non-disclosure. Where oversight bodies are perceived as an extension of the executive branch of government, their ability to serve as neutral arbiters is compromised. The minimal use of judicial review in RTI cases reinforces this problem – many refusals are not subject to an alternative source of independent review.

Administrative capacity is yet another structural gap. Many public officials do not have access to adequate organizations of records, as a result of limited digitization, and inadequate training, impeding the practical ability of the public to obtain information from them, even where there is a legal basis for the information's availability. These causes will tend to have a particularly negative effect on due to their marginalized status within most societies, thereby limiting the capacity of the right to information to uphold the principle of equality for all citizens, regardless of social status. Finally, the existence of an entrenched culture of secrecy in society constitutes a societal and cultural

gap. Many systems that have developed from colonial or authoritarianisms have tended to treat secrecy as a default mode of operation of state authority. Without sustained efforts to transform both administrative practices and create better levels of public awareness, legal reform on its own cannot rectify the problem, even if laws were written to ensure a right to information.

This book concludes that controlling the right to information, controlling the right to privacy, and governing state security do not operate as a zero-sum activity, nor are they eternally privileged interests over others. Rather, the process of regulating these three rights is a legal, context-sensitive process, controlled by principles, institutional safeguards, and democratic values.

The research evidences that properly managing the competing interests of the right to information, privacy and security starts with a recognition that RTI, privacy and security play a complementary role in a constitutional system. The RTI provides for transparent government, accountability; the right to privacy defends human dignity and personal autonomy; State security supports or defends collective interests and democracy. The existence of tension is not because of the incompatibility of these objectives, but because of the lack of coordination or rigidity in the respective legal frameworks in which the objectives are being pursued.

A proper approach to managing the competing interests requires treating restrictions to RTI as exceptions rather than creating a parallel regime of secrecy. Privacy claims must be evaluated by considering the public/private role of the affected individual and the relevance of the information to the public oversight. Similarly, any restrictions based upon security must be grounded in demonstrable risk, rather than speculating or symbolizing a risk. The lack of an evaluation process creates an

environment in which privacy and security are used as rhetorical cover to shield themselves from the application of law.

The research finds that, without external review, agencies do not possess adequate mechanisms for managing competing interests. Independent oversight agencies and the courts play an essential role in ensuring transparency and consistency in evaluating competing interests. Without independent review, balancing decisions will most likely reflect the institutional self-interest of an agency versus the constitutional principles of justice.

Not only will balancing not be static, but the balance will also change depending upon the context, subject matter, and societal conditions for the time in question. Because of the variability, legal regimes must provide for flexibility in the use of partial disclosures, redacting, delayed releases and public interest overrides.

Because of the lack of a clearly defined doctrine balancing privacy, security and RTI, there is a significant imbalance favoring secrecy in Bangladesh. It is therefore the position of this book that restoring the balance will not come from weakening the protections of any of the three rights, but will occur from the integration of all three rights through a transparent process of rule-based decision-making that recognizes the RTI as the foundation of governance in a democracy.

Recommendations for Legal Reform

The results of this research indicate a number of recommended legal and institutional reforms that will strengthen the effective realization of the right to information while providing appropriate safeguards for privacy and state security.

First, there is an urgent and pressing need for legislative precision in existing RTI frameworks. The key concepts that affect the realization of the right to information include national

security, personal protection of information and public interest - each must be defined in statutory terms. In addition, exemptions must be narrowly defined and supported by specific criteria of harm, to prevent restrictions on the right to information from being used when disclosure does not cause significant, disproportionate harm to legitimate interests.

Second, explicitly incorporating standards for balancing in RTI legislation is required, including necessity and proportionality. Decision-makers must be compelled by law to consider whether withholdings from the right to information are the least intrusive means available, even if the information is also subject to other restrictions, such as through partial disclosure, redaction or postponed disclosure. The establishment or enhancement of an override for public interest purposes is essential to prevent a mechanical application of exemptions and to promote democratic accountability.

Third, reforms must also address the harmonization between RTI and existing secrecy laws. Old statutes of secrecy must be updated and revised for harmony with current standards of transparency. RTI laws must have clear precedence over existing laws of secrecy when there is a conflict, subject only to narrowly defined exceptions.

Fourth, the establishment of institutional independence and ability to enforce RTI laws through independent oversight agencies (such as Information Commissions) is critical. Oversight agencies must have the capacity to make binding decisions with supporting rationale and to be challenged through the courts. Courts must play a more significant role in articulating balance principles and reviewing secret claims.

Fifth, effective legal reform is dependent upon administrative and cultural reforms. Capacity development, enhanced record-keeping, proactive disclosure obligations and public education must all be elements of forming a new institutional culture of

openness and transparency rather than secrecy. Without significant and ongoing supportive measures for formal legal reform, the intended results will not occur.

This book makes several original and substantive contributions to the academic and legal understanding of the right to information.

First, it offers a systematic and integrated analysis of RTI, privacy, and state security as interrelated legal principles rather than as isolated or competing domains. By examining these concepts together, the study moves beyond fragmented approaches and demonstrates that effective governance depends on their principled coexistence.

Second, the book contributes a context-sensitive comparative perspective, highlighting how similar legal norms produce divergent outcomes depending on institutional capacity, legal culture, and oversight mechanisms. This comparative analysis deepens understanding of why RTI reforms succeed in some jurisdictions while remaining fragile in others.

Third, the study provides a normative evaluation of balancing frameworks, particularly through its engagement with the Tshwane Principles. By situating these principles within broader international and domestic legal contexts, the book clarifies their relevance, limitations, and potential as a guiding model for democratic states.

Fourth, the detailed examination of Bangladesh adds a jurisdiction-specific contribution to the literature. The study not only documents legal provisions but critically assesses implementation challenges, structural gaps, and practical constraints. In doing so, it contributes to a more nuanced understanding of RTI in developing-state contexts.

Finally, the book contributes methodologically by demonstrating the value of doctrinal and analytical legal research

in addressing complex governance questions. Its integrative approach provides a framework that can be adapted for future research on transparency, accountability, and rights-based governance.

This book has argued that the right to information occupies a central position in contemporary democratic governance, functioning as both a substantive right and a procedural guarantee that enables accountability, participation, and the rule of law. Its relationship with privacy and state security is complex but not irreconcilable.

The study concludes that the primary challenge facing RTI regimes is not the existence of competing interests, but the absence of principled mechanisms to balance them. Where secrecy dominates, it is typically the result of vague laws, weak oversight, and institutional inertia rather than genuine necessity. Conversely, where transparency is governed by clear rules, independent review, and public interest reasoning, privacy and security can be protected without undermining openness.

Ultimately, the effectiveness of the right to information depends on a legal culture that treats transparency as the norm and secrecy as the exception. Achieving this balance requires more than legislative enactment; it demands sustained commitment to legal clarity, institutional accountability, and democratic values.

By articulating a coherent analytical framework and grounding it in comparative and national experience, this book seeks to contribute to that broader project. It affirms that a dignity-respecting, security-conscious, and transparency-oriented legal order is not only possible but essential for the legitimacy and resilience of democratic governance.

References

Ackerman, J. M., & Sandoval-Ballesteros, I. E. (2006). The global explosion of freedom of information laws. *Administrative Law Review, 58*(1), 85–130.

ARTICLE 19. (1996). *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*. London.

ARTICLE 19. (1999). *The public's right to know: Principles on freedom of information legislation*. London.

ARTICLE 19. (2006). *Freedom of expression and hate speech under international law*. London.

Balkin, J. M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review, 79*(1), 1–58.

Banisar, D. (2011). *The right to information and privacy: Balancing rights and managing conflicts*. World Bank Institute, Governance Working Paper Series, 5–20.

Bauhr, M., & Grimes, M. (2012). *What is government transparency? New measures and relevance for quality of government*. Quality of Government Institute Working Paper Series, 2012:16, 1–27.

Bennett, C. J. (2001). *Cookies, web bugs, webcams and cue cats*. Ethics and Information Technology, 3(3), 195–208.

Bertot, J. C., Jaeger, P. T., Shuler, J. A., Simmons, S. N., & Grimes, J. M. (2009). *Reconciling government documents and e-government*. Government Information Quarterly, 26(3), 433–436.

Birkinshaw, P. (2006). Freedom of information and openness: Fundamental human rights? *Administrative Law Review, 58*(1), 177–218.

Bluemel, E. B. (2004). The implications of formulating a human right to water. *Ecology Law Quarterly, 31*, 957–1005.

Buckland, B. S., & Wills, A. (2013). *Whistleblowing in the security sector*. In N. Ruzic & B. Medenica (Eds.), *Protection of whistleblowers* (pp. 1–34). Commissioner for Information of Public Importance and Personal Data Protection.

Bygrave, L. A. (2010). Privacy and data protection in an international perspective. *Scandinavian Studies in Law, 56*, 165–199.

Byrnes, A. (2010). Article 10 of the Convention on the Elimination of All Forms of Discrimination against Women. *Chinese Journal of International Law, 9*(2), 425–444.

Caidi, N., & Ross, A. (2005). *Information rights and national security*. Government Information Quarterly, 22(4), 663–684.

Calland, R. (2010). Access to information: Whose right and whose information? *Journal of Information Ethics, 19*(1), 1–14.

Cohen, J. E. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review, 52*(5), 1373–1438.

Coliver, S. (2012). *National security and the right to information*.

Committee on Economic, Social and Cultural Rights. (1999). *General Comment No. 12: The right to adequate food* (E/C.12/1999/5).

Committee on Economic, Social and Cultural Rights. (2002). *General Comment No. 15: The right to water* (E/C.12/2002/11).

Cook, R. J. (1994). State accountability under the Convention on the Elimination of All Forms of Discrimination against Women. *Human Rights Quarterly, 16*(3), 507–543.

Council of Europe, European Court of Human Rights, Research Division. (2013). *National security and European case law*. Council of Europe.

Craig, P. (2012). Proportionality, rationality and review. *New Zealand Law Review*, 265–299.

Cuillier, D., & Piotrowski, S. J. (2009). Internet information-seeking and its relation to support for access to government records. *Government Information Quarterly, 26*(3), 441–449.

de Vries, K., Bellanova, R., & De Hert, P. (2010, May). *Proportionality overrides unlimited surveillance: The German Constitutional Court judgment on data retention*.

Detrick, S. (1999). *A commentary on the United Nations Convention on the Rights of the Child*. Martinus Nijhoff Publishers.

Fenster, M. *The transparency fix: Advocating legal rights and their alternatives in the pursuit of a visible state*.

Fox, J. (2007). *The uncertain relationship between transparency and accountability*. Development in Practice, 17(4–5), 663–671.

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal, 89*(3), 421–471.

Gormley, K. (1992). *One hundred years of privacy*. Wisconsin Law Review, 1335–1422.

Grimes, M. (2008). *The conditions of successful civil society involvement in combating corruption: A survey of case study evidence* (QoG Working Paper Series, 2008:22). The Quality of Government Institute.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., & Nouwt, S. (Eds.). (2009). *Reinventing data protection?* Springer Netherlands.

Hoq, K. M. G. (2012). *Information ethics*. Philosophy and Progress, LI–LII, 37–48.

Hoq, K. M. G. (2013). Right to information: The roles and contributions of information professionals of Bangladesh. *Philosophy and Progress, 53–54*, 44–58.

Human Rights Committee. (1988). *General Comment No. 16: Article 17 (Right to Privacy)*, UN Doc. HRI/GEN/1/Rev.1.

Human Rights Committee. (2011). *General comment No. 34: Article 19: Freedoms of opinion and expression* (CCPR/C/GC/34). United Nations.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review*, 17(1), 83–119.

Hutchinson, T., & Duncan, N. (2012). *Doctrinal legal research*. Deakin Law Review, 17(1), 83–119.

Johannesburg Principles on National Security, Freedom of Expression and Access to Information. (1995).

Joseph, S., Schultz, J., & Castan, M. (2004). *The International Covenant on Civil and Political Rights: Cases, materials, and commentary*. Oxford University Press.

Karim, M. F. (2013). *Implementation of the Right to Information Act (RTI-2009) in the selected upazilas of Mymensingh District* (master's book). Institute of Governance Studies (IGS), BRAC University, Dhaka.

Kinkopf, N. (n.d.). *The state secrets problem: Can Congress fix it?*

La Rue, F. (2013). *Promotion and protection of the right to freedom of opinion and expression*. UN General Assembly (A/68/362).

Lansdown, G. (2005). The evolving capacities of the child. *International Journal of Children's Rights, 13*(3), 297–328.

Lindstedt, C., & Naurin, D. (2010). Transparency is not enough: Making transparency effective in reducing corruption. *International Political Science Review, 31*(3), 301–322.

London, L. (2008). *What is a human-rights based approach to health?* Health and Human Rights, 10(1), 65–80.

Lyons, C. N. (2007). *The state secrets privilege: Expanding its scope through government misuse.*

McDonagh, M. (2013). *The right to information in international human rights law*. Human Rights Law Review, 13(1), 25–55.

Mendel, T. (2003). *Freedom of information as an internationally protected human right*. Comparative Media Law Journal, 1(1), 1–28.

Mendel, T. (2003). *Freedom of information: A comparative legal survey*. UNESCO / World Bank.

Mendel, T. (n.d.). *Restricting freedom of expression: Standards and principles*. Background paper for meetings hosted by the UN Special Rapporteur on Freedom of Opinion and Expression.

Murad, M. H., & Hoque, K. A. (2011). The Right to Information Act in Bangladesh: An analysis in the light of Johannesburg Principles of Freedom of Information Legislation. *IIUC Studies, 7*, 73–90.

Narula, S. (2006). The right to food: Holding global actors accountable under international law. *Columbia Journal of Transnational Law, 44*, 691–800.

Nathan, L. (2009). *Lighting up the intelligence community: A democratic approach to intelligence secrecy and openness*.

Nigar, M. (2013). Right to Information (RTI) in Bangladesh: Looking within and beyond. *Journal of Law, Policy and Globalization, 13*, 1–12.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Nowak, M. (2005). *U.N. Covenant on Civil and Political Rights: CCPR commentary*. N.P. Engel Verlag.

Open Society Foundations. (2013). *The global principles on national security and the right to information (Tshwane Principles)*.

Open Society Justice Initiative. (2013a). *Understanding the global principles on national security and the right to information (The Tshwane Principles)*. Open Society Foundations.

Open Society Justice Initiative. (2013b). *Global principles on national security and the right to information (The Tshwane Principles)*. Open Society Foundations.

Organization for Security and Co-operation in Europe (OSCE). (2012). *Brief on access to information*. Vienna.

Parliamentary Assembly of the Council of Europe. (2013). *National security and access to information* (Doc. 13293).

Peled, R., & Rabin, Y. (2011). The constitutional right to information. *Columbia Human Rights Law Review*, 42(2), 357–398.

Peled, R., & Rabin, Y. (2010, November 10). *The constitutional right to information*. SSRN. https://ssrn.com/abstract=1706606

Pozen, D. E. (2009). Deep secrecy. *Stanford Law Review*, 62, 257–339.

Pozen, D. E. (2013). *The leaky Leviathan: Why the government condemns and condones unlawful disclosures of information*. Harvard Law Review, 127(2), 512–635.

Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383–423.

PSWG3. *Privacy and data protection as fundamental rights: A narrative*. https://globalprivacyassembly.com/wp-content/uploads/2022/05/PSWG3-Narrative-Final.pdf

Redress Trust. (2006). *Jurisprudence of the Human Rights Committee*. In *Seeking remedies for torture victims* (pp. 155–203).

Relly, J. E., & Sabharwal, M. (2009). Perceptions of transparency of government policymaking: A cross-national study. *Government Information Quarterly*, 26(1), 148–157.

Right to Information Act, 2009 Bangladesh, Ministry of Law, Government of Bangladesh.

Roberts, A. (2004). National security and open government. *Georgetown Public Policy Review, 9*(2), 69–85.

Roberts, A. S. (2005). Spin control and freedom of information: Lessons for the United Kingdom from Canada. *Public Administration*, 83(1), 1–23.

Roberts, A. S. (2006). *Blacked out: Government secrecy in the information age*. Cambridge University Press.

Roberts, A. S. (2010). A great and revolutionary law? The first four years of India's Right to Information Act. *Public Administration Review*, revised version, 1–32.

Rubenfeld, J. (1989). The right of privacy. *Harvard Law Review, 102*(4), 737–807.

Schwartz, P. M. (1995). European data protection law and restrictions on international data flows. *Iowa Law Review, 80*, 471–522.

Sen, A. (1999). Democracy as a universal value. *Journal of Democracy, 10*(3), 3–17.

Siddiqui, M. S. (2009). *Right to Information Act, 2009*. Government of Bangladesh.

Stone, G. R. (2011). Secrecy and self-governance. *New York Law School Law Review, 56*, 81–130.

Subrahmanyam, A. (2002). Transparency in administration and protection of human rights. *Journal of the Indian Law Institute, 44*(2), 258–268.

Sultana, T. (2012). *Right to Information Act, 2009 (Bangladesh)*. Northern University Journal of Law, 3, 63–75.

Szekely, I. (2009). Freedom of information versus privacy: Friends or foes? In S. Gutwirth et al. (Eds.), *Reinventing data protection?* (pp. 293–316). Springer.

Thomson, J. J. (1975). The right to privacy. *Philosophy & Public Affairs, 4*(4), 295–314.

Tomasevski, K. (2001). *Human rights obligations: Making education available, accessible, acceptable and adaptable*. Right to Education Primers No. 3.

Turle, M. (2007). Freedom of information and data protection law – A conflict or reconciliation? *Computer Law & Security Report*, 23(6), 514–522.

United Nations General Assembly. (1946). *Resolution 59(I): Calling of an international conference on freedom of information*.

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

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

United Nations. (1979). *Convention on the Elimination of All Forms of Discrimination against Women*.

United Nations. (1989). *Convention on the Rights of the Child*.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.

Wells, H. (n.d.). *The state secrets privilege: Overuse causing unintended consequences.*

Whitman, J. Q. (2004). The two Western cultures of privacy: Dignity versus liberty. *Yale Law Journal, 113*, 1151–1221.

Wolfers, A. (1952). "National security" as an ambiguous symbol. *Political Science Quarterly, 67*(4), 481–502.

Worthy, B. (2010). More open but not more trusted? The effect of the Freedom of Information Act 2000 on the United Kingdom central government. *Governance, 23*(4), 561–582.