Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation

Allison Carnegie (Columbia University) and Austin Carson (University of Chicago)

November 19, 2019

Contents

List of Figures

List of Tables

Chapter 1

Introduction

War crimes committed in the former Yugoslavia in the 1990s led to a chorus of calls for punishment of the perpetrators. Accountability advocates hoped to use international law to provide justice for the victims, deter future war crimes, and facilitate peace. A key challenge, however, was obtaining conclusive evidence. Locating mass graves and documenting who gave specific orders was often only possible by resorting to national intelligence agencies. Photos from satellites or signals intercepts, in some instances, could furnish proof of wrongdoing and facilitate the international community's pursuit of justice.[1] Yet disclosing intelligence carried a high cost: doing so could inform current and future intelligence targets about sensitive collection methods. Germany's release of drone-based photographs, for example, alerted Serbian leaders allowing them "to return to the killing fields and destroy the mass graves in order to remove and scatter the evidence."[2] Such evasion could undermine the goal of accountability or invite other, unrelated security risks. Reluctance to take on such risks left the international community "hampered by a lack of information about the

[1]Branigin, William. "U.S. Evidence Enhances Case Against Milosevic." *Washington Post.* May 28, 1999; Manning 2000, 1, 12, 16.

[2]Scheffer 2012, 274.

Yugoslav high command that only government agencies can supply."[3]

Due to these difficulties, one could be forgiven for dismissing the practicality of relying on intelligence to further transnational justice or other multilateral goals. Yet the experience of the International Criminal Tribunal for the Former Yugoslavia (ICTY) suggests otherwise. The ICTY developed procedures to "protect confidential information obtained by the Prosecutor," which allowed the Prosecutor's office to "offer new assurances to states" and earned their "trust and confidence."[4] American leaders, who had been at the center of "a persistent tug of war over classified evidence," disclosed key insights derived from intelligence to the ICTY through these channels, facilitating indictments of top leaders including Slobodan Milosevic.[5] Beyond strengthening accountability for war crimes in Yugoslavia,[6] the integration of intelligence at the ICTY served as a "laboratory for learning about the implications of using and protecting national security evidence in international criminal trials" and influenced the design of the International Criminal Court.[7]

Yet despite its potential importance, we know little about the nature of sensitive information in global governance, how IOs might integrate it, and the effects of such efforts. This is particularly striking due to the ubiquity of sensitive information in modern society, and the practical difficulties that such information can raise. For example, is it possible to share information to stop a spreading disease without compromising the privacy of health records? Can leaders hold industries accountable for their pollution without disclosing the proprietary information of the firms involved? Can the international community give peacekeepers high

[3]Marise Simons. "U.S. and Britain Vow to Give War Court Data on Top Yugoslavs." *New York Times*, April 18, 1999.

[4]Moranchek 2006, 484. These reforms included increased closed witness hearings and the use of intelligence as lead evidence, as we detail in subsequent chapters.

[5]Branigin, "U.S. Evidence Enhances Case Against Milosevic." Moranchek (2006, 485) notes that "although the United States provides the most dramatic example of a country's hesitation to provide secret evidence to international tribunals without protections, other powerful Western countries, such as the United Kingdom and France, have expressed similar concerns in other fora."

[6]Bosco 2013, 115.

[7]Moranchek 2006, 497.

quality information to monitor a ceasefire without revealing a governments sources?

This book sheds light on these issues. In doing so we address two central research questions. First, what factors explain whether states and firms disclose their sensitive information to address questions of compliance? Second, what impact does sensitive information have on the effectiveness of international organizations and the cooperative goals they are designed to further? Our answers address several longstanding debates in the study of International Relations. These include the barriers to cooperation that states face under anarchy, how formal international organizations mitigate such barriers, and the sources of power and uncertainty in international politics. They also have important policy implications, suggesting how the international community may more effectively hold leaders accountable for war crimes, resolve thorny trade disputes, identify hidden nuclear weapons facilities, and uphold rules for foreign investment.

More broadly, our framework provides new insights into when global governance works and whether this can be consistent with inclusive, transparent procedures. International organizations are a defining feature of the liberal international order, and represent a critical venue for diplomatic consultation. Yet, in the past ten years, these institutions have been under severe duress. This book suggests ways to make IOs more effective and responsive by providing insights into how IOs work and how information circulates within them.

To do so, we disaggregate "information" into two types: sensitive and non-sensitive. Sensitive information refers to private information whose wide dissemination would allow changes in behavior that are harmful to the discloser by other state and non-state actors. We asses the factors that influence how states handle sensitive information when it bears on international cooperation, theorizing the incentives and disincentives that determine its disclosure. Absent some remedy, we show that states and firms typically react to these dilemmas by withholding it. We then analyze how IOs can be equipped to protect and use sensitive information, offering informed actors a third option in addition to staying silent

and going public. Our theory therefore highlights the importance of secrecy in IOs. In doing so, we build on the recognition that institutions affect what states and other actors are willing to do with compliance-related information.[8] Moreover, linking sensitive information, confidentiality, and IOs allows for fresh insights into the pervasiveness of uncertainty under anarchy and the difficulties of achieving cooperative goals.

More specifically, we argue that anticipated adaptations to sensitive information can deter the disclosure of key insights about compliance with international rules. This, in turn, can allow violations to go undetected and unpunished, depressing efforts at international cooperation. In a vacuum, states and firms have good reasons to share their insights about compliance with international rules and agreements, either to clear their own names or to incriminate others in line with their political and economic interests. Yet when those insights are based on sensitive information, their revelation can allow other actors to adapt in ways that harm the discloser. This tension creates what we call a "disclosure dilemma."

We focus on two manifestations of this problem. First, if a state widely disseminates insights based on intelligence, it may expose its sources and methods and jeopardize future efforts to collect such information. Similarly, if a firm or government widely distributes sensitive firm-specific economic details, market competitors can react in ways that jeopardize the firm's commercial prospects. In both cases, simply omitting the sensitive portions of the information can moot its value and undermine the credibility of its claims due to firms' and states' incentives to lie.

However, we argue that IOs can mitigate these dilemmas. The traditional view of IOs as information transmission belts would, if anything, sharpen the damage from disclosing sensitive information. However, if an IO develops a secrecy capability – what we refer to as a "confidentiality system" – then states and firms can disclose their information directly and exclusively to an institution. The IO can then receive the sensitive information, vet

[8] Keohane 1984*a*.

it, and widely share its conclusions, all while protecting the sensitive details. Doing so can improve states' abilities to meet common goals by drawing out information that these actors would otherwise keep behind national borders and closed corporate doors. While we posit that properly equipped IOs constitute a potential remedy for these dilemmas, we emphasize that this success is hard-won, as IOs must develop and maintain reputations for strong information security.

At the same time, an institutional solution to disclosure dilemmas can potentially create new problems. Designing IOs to accommodate sensitive details requires accepting some level of institutional secrecy, which is in tension with the normative goal of making global governance institutions more transparent.[9] In addition, confidentiality systems cannot stop governments from disclosing sensitive information to an IO in a selective fashion. While past scholarship has focused on how states exert power via leadership positions, bribery, and informal procedures, we show how states can turn the spigot of sensitive information on and off to shape who and what gets scrutinized.

In the chapters that follow, we apply these ideas to a range of issue areas using elite interviews, original archival research, and quantitative empirical tests that draw on newly collected data. In the domains of war crimes, international trade, nuclear proliferation, and foreign investment, we assess how variation in IOs' confidentiality systems interacts with informed actors' vulnerability to adaptation problems and potential assumption of incrimination benefits to impact the frequency of sensitive information disclosures. We then show how this information provision can impact the success of efforts to cooperate. The result is a novel story about how equipping international organizations with secrecy can allow the international community to harness the unique but sensitive insights of both states and firms.

[9] E.g. Grigorescu 2003, 2007*a*; Koppell 2010; Tallberg, Sommerer and Squatrito 2013; Tallberg et al. 2014; Grigorescu 2015.

1.1 The Puzzling Persistence of Secrecy

A core motivation of this book is to help make sense of the otherwise puzzling persistence of secrecy in IOs, which has been largely overlooked by scholars and practitioners. A dominant view among scholars is that IOs are tools that ease access to compliance information. These scholars have shown that IOs can facilitate cooperation by gathering information and receiving submissions from member-states and non-state actors, and then releasing these details widely.[10] Doing so helps to ensure that defections from cooperative agreements are identified, commonly known, and punished through either centralized or decentralized methods, magnifying reputational costs and other penalties and empowering domestic and transnational pressure groups.[11] Influential work in this area has argued that IOs must guarantee that information "is made available, more or less equally to all members"[12] and that IOs serve "as a repository and communicator of information."[13]

Outside of the academy, global governance institutions have been the object of strong demands for greater transparency. While secrecy had long been the norm for diplomacy and multilateralism,[14] a transparency norm in global governance emerged in the interwar period following World War I. The American president Woodrow Wilson famously called for "open covenants of peace, openly arrived at" as part of his broad repudiation of traditional power politics. Yet it was only with the end of the Cold War that the apex of transparency in domestic and global governance was reached. Since 1991, IOs from the WTO to NATO have developed new policies to improve public access to information about their deliberations, judgments, and activities.[15] As Keohane (2005, 49) notes, "the decision-making processes of many multilateral organizations have become remarkably transparent" to the extent that

[10] Mitchell 1998; Dai 2002*a*.
[11] Mansfield, Milner and Rosendorff 2002; Dai 2002*a*, 2005; Thompson 2006*a*; Chapman 2007; Fang 2008.
[12] Keohane 1984*a*, 94
[13] Dai 2002*a*, 411.
[14] Colson 2008.
[15] Grigorescu 2007*b*, 625.

"they now compare well to the decision-making processes of most governments."

Despite this trend, we find a puzzling persistence of a specific secrecy function in IOs across the international landscape. The ICTY's integration of national intelligence is, in this sense, far from unusual. Sensitive information stored confidentially in IOs has been used to better implement peacekeeping missions, combat drug trafficking, enforce sanctions regimes, trace terrorism financing, and address environmental degradation. The charter for the Organization for the Prohibition of Chemical Weapons stipulates that it "shall take every precaution to protect the confidentiality of information on civil and military activities and facilities coming to its knowledge."[16] The International Narcotics Control Board assures members that data submitted about private sector trade in precursor chemicals will not expose "industrial, business, commercial or professional secrets or trade processes."[17] The International Monetary Fund developed a three-tiered classification system for highly sensitive banking-related documents to better assess financial systems' health.[18] The secretariat for the 1989 Montreal Protocol on emissions of chlorofluorocarbons is designed to "protect the confidentiality of information" because members' submissions may feature "sensitive technical and commercially valuable information."[19] Our own data collection, described in Chapter 3, suggests that almost half of international organizations have some kind of confidentiality process to handle sensitive information.

What explains this persistence – and in many cases expansion – of secrecy in IOs? Why have institutions like the World Bank and the IAEA simultaneously opened up archives and deliberations while *strengthening* their ability to receive and protect sensitive information? Answering these questions calls for a theory of how integrating sensitive information can

[16]Article VIII, Chemical Weapons Convention.

[17]UN General Assembly Resolution S-20/4 ("Measures to enhance international cooperation to counter the world drug problem"), Section I, Subsection B ("Information exchange"), Para 7.

[18]Articles of Agreement of the International Monetary Fund, Article V, Section 2(B), "Confidentiality Protocol - Protection Of Sensitive Information In The Financial Sector Assessment Program."

[19]Handl 1997, 40.

help an IO to fulfill its mission, and the role that secrecy plays in eliciting the disclosure of such information.

1.2 The Problem: Disclosure Dilemmas

The first step in answering these questions is rethinking the nature of the information problems that leaders and economic actors face when they seek to cooperate on international issues. Many forms of international cooperation require timely and accurate information about compliance, particularly due to fundamental conditions of mistrust and fear in the international system.[20] In particular, states and firms must be able to determine whether governments are cheating on their agreements in order to punish these infractions and deter future breaches. If states' violations are not detected, violators can exploit compliant states, which can discourage cooperation from occurring in the first place.[21] Scholars and practitioners argue that improved information about compliance via IOs facilitates cooperative efforts;[22] however, such information can be difficult to obtain. Detecting non-compliance often requires specialized techniques or knowledge that only specific states or non-state actors have access to, especially because rule breakers typically try to hide their transgressions.[23] For example, insights into well-hidden nuclear facilities may only be available to intelligence bureaucracies, or evidence of damage from a foreign trade barrier may be found in detailed internal documents from firms in affected sectors.

Informed actors thus often face decisions about whether to reveal their compliance-related information. Sharing sensitive information might help to demonstrate innocence regarding an accusation of trade discrimination or protect a country's reputation for respecting foreign

[20] Booth and Wheeler 2007.

[21] Keohane 1984*a*; Axelrod and Keohane 1985; Milgrom, North et al. 1990*b*; Mitchell 1998; Koremenos, Lipson and Snidal 2001; Dai 2002*a*; Lindley 2004; Carrubba 2005; Voeten 2005; Thompson 2006*b*; Lindley 2007; Guzman 2008.

[22] Dai 2002*a*.

[23] Hafner-Burton 2008*a*.

investments. Alternatively, sensitive information might substantiate claims of a competitor or rival's wrong-doing. National intelligence disclosures could show that a leader authorized an atrocity during a war, thereby facilitating multilateral penalties, ending the atrocities, or deterring future acts. We call these compliance-related advantages "incrimination benefits." While sensitive information is sometimes irrelevant to questions of compliance, or its disclosure may be harmful if it incriminates an informed state's ally or the informed state itself, it is often helpful for maintaining cooperative agreements and settling compliance controversies. In such cases, disclosure dilemmas can arise.

At the same time, revealing sensitive information often has downsides. Publicly circulating intelligence or private firm material can empower other actors to make adjustments that harm the discloser, which we refer to as "adaptation costs." For example, if a government publicizes satellite photos of another country's concealed nuclear site, other proliferators or non-state actors that it has a keen interest in monitoring may move their activities underground to avoid future detection. Alternatively, publicly revealing details of a bank's loan portfolio to allow an evaluation of a country's financial sector health could cause a bank run or other adverse market reactions. These potential adverse effects are what make such information "sensitive."[24] Such harmful adaptations do not always follow the wide dissemination of sensitive information, such as when other actors cannot change quickly or adapt regardless of whether sharing takes place. Thus, a disclosure dilemma is only present when countries face meaningful costs and benefits from from disclosing sensitive information that is relevant to compliance issues, as shown in Figure 1.1. The trade-off between adaptation costs and incrimination benefits in such cases is difficult to avoid. For example, removing sensitive details from a disclosure can reduce adaptation costs but also reduces the benefits by creating credibility problems.

[24]This terminology builds on Grando (2009, 276), who defines confidential information in the international trade setting as "non-public business or proprietary information and government information which is not accessible to the public."

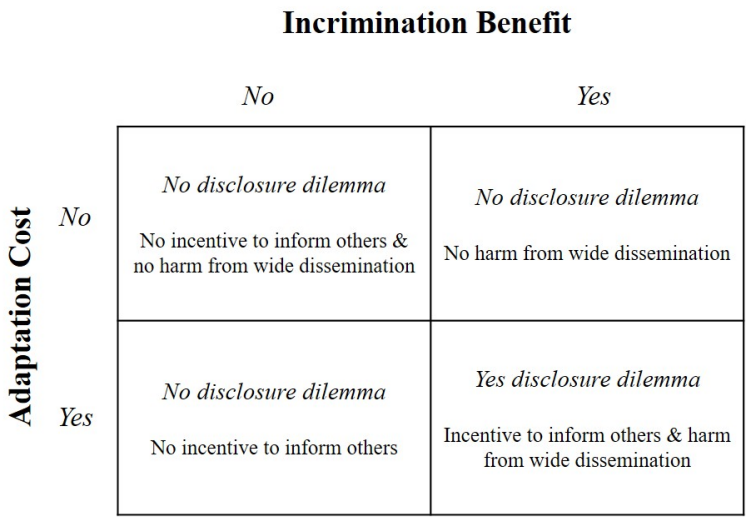


Figure 1.1: Conditions for Disclosure Dilemmas

1.3 The Solution: IOs and Sensitive Information

We argue that international organizations, if properly designed, can ameliorate disclosure dilemmas by adopting a confidentiality system, which allows an IO to directly receive and vet sensitive information. Countries and firms reveal sensitive information when the benefits of its disclosure outweigh the costs. By reducing the costs, an IO with a confidentiality system can make it easier for informed actors to share these unique insights when they otherwise might not. The more an IO lowers the cost, the more it can solve these dilemmas. Eliciting such disclosures, moreover, helps clarify compliance questions. For instance, receiving firm-specific details might help an IO to adjudicate trade disputes; integrating intelligence findings into its assessment can help an IO link leaders to war crimes.

To perform this function effectively, an IO must develop an organizational capacity for securely storing information and preventing leaks, which mitigates the adaptation costs associated with revealing sensitive details.[25] For example, an IO may need to develop a system that identifies and regulates access to sensitive documents, categorizing them by their degree

[25]Geser 1992; Gibson 2014.

of sensitivity and developing policies that pertain to different levels of access. The IO may also require measures to securely store data and documents, using physical lock-and-key systems for "hard" data and encryption and other information technology for "soft" data. These measures may also include personnel rules that establish how employees should handle sensitive information and penalties for unauthorized disclosures.[26] Such organizational changes, often driven and supported by personal relationships between state and secretariat leaders, can build trust that disclosures will be protected.[27] International organizations as leak-proof storehouses for information may seem implausible, yet a broad finding of the book is that protections for sensitive information are often surprisingly robust in IOs like the IAEA or WTO. This is because IOs can develop cultures that reward secrecy and can adopt physical and organizational measures to limit information access to small groups.

Once IOs receive sensitive information, they can assess its validity, which avoids the credibility problem that arises if a state or firm only reveals its conclusions. Vetting involves secretariat experts applying their technical knowledge and other sources of information to reach conclusions about the accuracy of a claim.[28] Because sensitive details are withheld from other actors, an IO's reputation for technocratic and unbiased judgment is important.[29] After vetting a disclosure that was made in confidence, an IO can combine such information with other sources to reach a conclusion and circulate it widely.

While we argue that properly equipped IOs *can* mitigate disclosure dilemmas, this is not always the case. First, states and firms may not choose to use a confidential disclosure option. We argue that states tend to withhold intelligence from IOs regarding allies, even when a confidential route exists, giving rise to a selective disclosure pattern. Second, states

[26] Pozen 2013; Sagar 2016.

[27] Wheeler 2018.

[28] Some scholars argue that third party mediators including IOs can validate information about compliance in conflict settings, though the specific importance of protecting sensitive information has not been developed at length. See, for example, Kydd 2006; Lindley 2007; Mattes and Savun 2010.

[29] On the role of IOs in legitimizing policy proposals, see Voeten 2005; Thompson 2006*a*; Chapman 2007.

do not always equip IOs to deal with disclosure dilemmas. Developing the procedures for confidentiality can be difficult, as we detail in the following chapters. The design of international institutions is generally path dependent, especially when considering a politically and logistically challenging function like secrecy.[30] As a result, disclosure dilemmas can go unaddressed by IOs for years or even decades. These same concerns also explain why states do not delegate sensitive information collection to IOs. Governments are typically loathe to delegate the level of intrusive information collection and legal authority that is required to do so.

1.4 Empirical Approach

We use our theoretical framework to address two central research questions: What factors explain whether states and firms disclose sensitive information, and what impact does this information have on international cooperation? We derive two primary empirical expectations from our theory, which we assess in four empirical chapters.

First, our theory outlines conditions under which states and firms with sensitive information should disclose it, highlighting the importance of institutions and, for states, geopolitical self-interest. Our claims suggest that governments and firms should disclose sensitive information only if an IO is equipped with a credible confidentiality system. Even then, states' disclosures should also be influenced by their geopolitical self-interest. Similarly, our theory suggests that a shift from confidentiality to public accessibility in an IO should deter sensitive disclosures.

Second, our theory has implications for international cooperation. The successful solicitation of sensitive information from a firm or government should provide IOs with new insights about compliance-related questions. The practical problem of identifying and doc-

[30] E.g. Pierson 2011.

umenting non-compliance and responding to violations should be eased by the addition of a new source of information. In the intelligence context, disclosures should on average provide greater clarity about the existence of violations and specific actors' culpability. Governments, rebels, terrorist groups, and drug traffickers often go to great lengths to limit their detection; shared intelligence should counteract such evasion techniques.[31] For compliance questions involving firm activity, under-the-hood documents and data can document violations and quantify financial damages. These contributions cut across economic and security issue areas; for example, confidentiality protections for firms may facilitate security cooperation goals. The chemical production companies whose activities are monitored as part of a chemical weapons ban, for example, should more honestly report production figures if they trust that commercially sensitive details will be protected.[32]

Later chapters adapt these hypotheses to each of four empirical domains: nuclear proliferation, trade, war crimes, and investment. For example, Chapter 4 assesses whether confidentiality reforms in war crimes tribunals increased the disclosure of sensitive intelligence details during indictments and trials of leaders in the former Yugoslavia and Rwanda. It also analyzes whether and how intelligence details improved the likelihood of indictments, apprehension, and convictions of war criminals.[33] We discuss the central features and distinguishing characteristics of each of the four empirical applications in Chapter 2.

1.5 Downstream Consequences

While we argue that adopting confidentiality systems to ameliorate disclosure dilemmas increases information sharing and cooperation, this solution is not a cure-all. In particular,

[31] On norm and law evasion, see Búzás 2017.

[32] E.g. Krepon 1992.

[33] The chapter specifically analyzes sensitive information about violations of international criminal law governing wartime atrocities. The prosecution of these crimes lies at the intersection of international law, human rights, and security studies (Rudolph 2001; Morrow 2007; Hafner-Burton 2012; Morrow 2014).

allowing IOs to keep secrets can create new challenges for global governance. Throughout the book, we return to two potential downstream consequences – regarding both transparency and power – that can have important normative and practical implications.

First, adding confidentiality systems to IOs diminishes institutional transparency. Our theory posits that a necessary condition for integrating sensitive information is an organizational ability to protect particular kinds of information from unauthorized access. Excluded audiences may include some secretariat personnel within IOs, other member-states, and external audiences like NGOs and publics. Confidentiality systems in IOs therefore limit what other member-states see and the feasibility of outsider participation. As our later chapters describe, measures to secure information can inject public-facing documents with deletions or redactions of sensitive details. Limits on physical access and documentary transparency can place IOs in difficult positions, as they risk running afoul of expectations that institutions – local, national, and global – are transparent and accountable. However, since they are often necessary for resolving disclosure dilemmas, we argue that our framework paradoxically requires states to trade-off one kind of transparency for another. In other words, while confidentiality systems *decrease* the observability of organizational decisions and activities, they *increase* the observability of compliance with international rules and norms.

A second downstream effect relates to power. As we noted previously, informed states and firms retain discretion about whether to take advantage of the opportunity to provide confidential disclosures. While political relationships likely do not strongly shape firms' decisions, since firms primarily care about the bottom line, states are prone to factoring in their relationship with the suspected violator. We find that states often selectively disclose what they know to IOs, which provides the informed actor with a subtle tool of power. While many scholars argue that power in IOs is determined by which states hold key positions within these bodies, provide funds for their operations, bribe other members, or exploit

their informal procedures,[34] we demonstrate that informed states use sensitive information disclosures to influence the information landscape and shape outcomes. We return to both themes in Chapters 2 and 8.

1.6 Contributions

This book offers a unified, multi-method approach to understanding international cooperation that spans economic and security domains. While these arenas are typically treated separately in the field of international relations, we bridge this divide, and in doing so, provide theoretical, empirical, normative, and practical contributions.

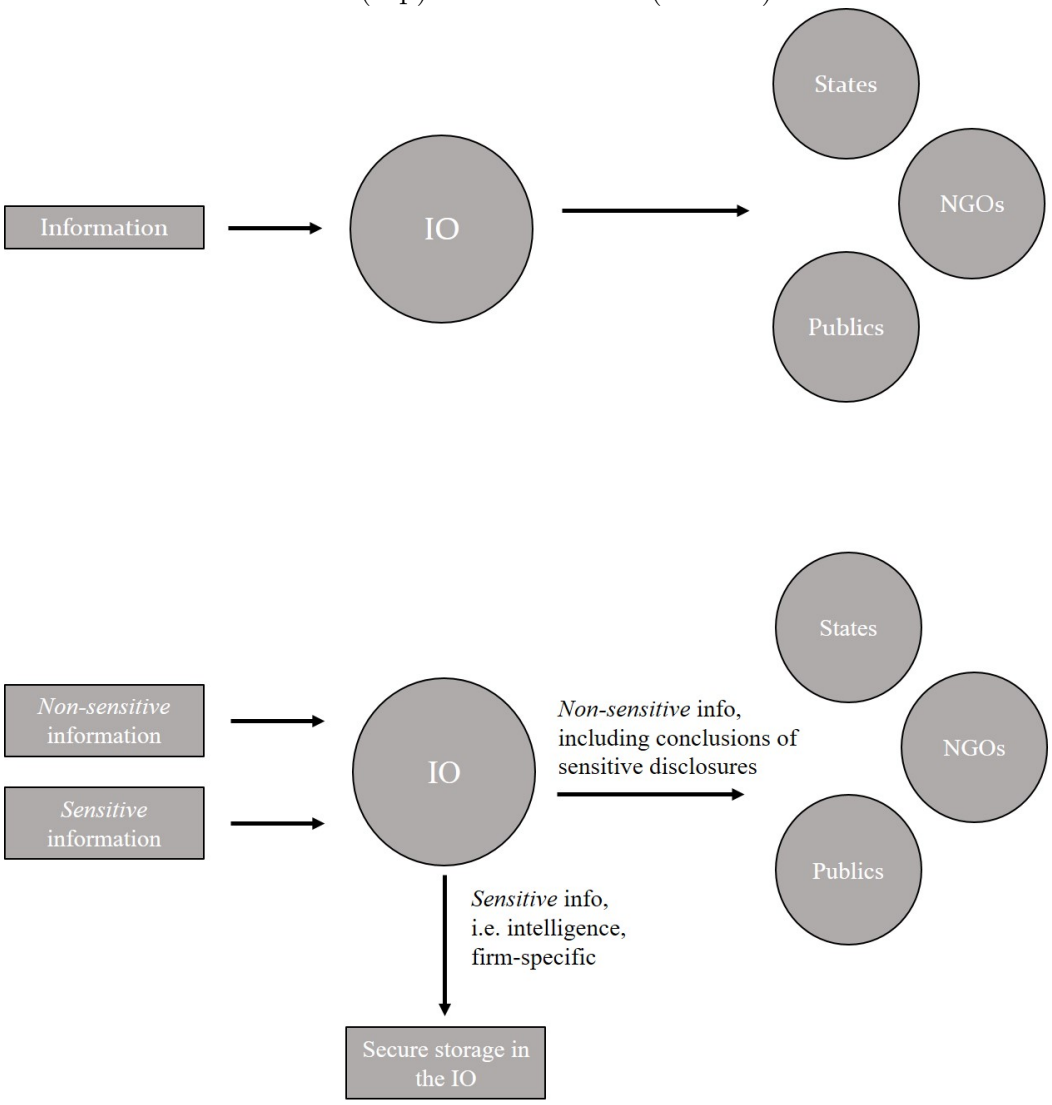
1.6.1 Theoretical

The book most directly addresses debates about information, cooperation, and institutions. Our theory and findings complicate the traditional view of IOs as mechanisms for easing access to compliance information through the wide dissemination of information. As we explained previously, scholars typically conceive of IOs as bodies that encourage cooperation by gathering information and then distributing it widely. Indeed, while IOs may also improve cooperation by reducing transaction costs or acting as commitment devices, information provision is typically an important element of these accounts.[35] However, while we do not dispute that IOs often increase cooperation in this manner for *non*-sensitive information, we show that *sensitive* information must be treated differently. Figure 1.2 captures this contrast. The top shows the conventional view of IOs as information transmission belts. Information that an IO receives is disseminated widely to states, publics, and other interested actors. The bottom features our model, which emphasizes the importance of secure storage for

[34] Tallberg 2003; Broz and Hawes 2006; Dreher, Nunnenkamp and Thiele 2008; Stone 2011.

[35] See Keohane 1984*a*; Fearon 1998; North and Weingast 1989; Carnegie 2014, 2015; Axelrod and Keohane 1985; Milgrom, North et al. 1990*b*; Mitchell 1998; Koremenos, Lipson and Snidal 2001; Carrubba 2005; Voeten 2005; Thompson 2006*a*; Guzman 2008.

Figure 1.2: Traditional Model (top) vs. Our Model (bottom) of IOs and Information



sensitive details. Our model acknowledges that IOs play a key dissemination role for non-sensitive information and conclusions that are based on sensitive submissions, yet highlights the importance of secure storage for sensitive details. This figure helps to underscore an important theme of the book: IOs serving the traditional information transmission belt function actually *sharpen* the adaptation costs from sensitive information, deterring countries and firms from disclosing it in the first place. Building a confidentiality system is necessary to avoid these effects.

In addition, the mechanism we develop differs from past scholarship on private bargaining. Not all scholars emphasize IOs' information provision function. Some have built on theories of

the value of private settings for bargaining to suggest that closed-door discussions in IOs may facilitate diplomatic compromises. Shielding diplomats from domestic scrutiny eliminates temptations to posture[36] and productively avoids constraints from two-level games.Putnam 1988, 445. In contrast, we argue that confidentiality systems in IOs help with enforcement rather than bargaining.[37] Here secrecy for compliance-related submissions by states or firms can be an important ingredient in achieving successful cooperation.

Beyond this framework's theoretical contributions to institutions and information, our book also addresses the burgeoning literature on secrecy in the international system. Existing work has largely focused on the logics for and consequences of secrecy at the state level.[38] Less common has been theoretical and empirical analyses of secrecy in regional or global governance.[39] This book identifies a novel secrecy-related function which allows IOs, and by extension states, to better identify non-compliance and meet cooperative goals. In doing so, we show that IOs can play critical roles in some of the most difficult, highly-charged international settings. Skeptics of institutions have argued that IOs may matter for issues of "low politics" but take a back seat to material power in matters of national security.[40] However, we show that IOs can address, for example, high-stakes trade disputes and clandestine nuclear proliferation programs. More broadly, we discuss how moving beyond state-centric secrecy research constitutes a promising avenue for future research.

Finally, our framework and findings provide new insights into a central issue that cuts across international relations: the problem of uncertainty under anarchy. Our concepts of sensitive information, adaptation costs, and disclosure dilemmas join a long tradition

[36]Stasavage 2004*a*.
[37]Fearon 1998.
[38]E.g. Yarhi-Milo 2013; Carson 2016; Spaniel and Poznansky 2018; Banka and Quinn 2018; Finel and Lord 1999*a*. See also work on the rise of transparency norms within specific states, especially the United States, e.g. Schudson 2015; Pozen 2018; Epstein 2019, along with work on leaks e.g. Castle and Pelc 2017; Kydd and Saunders 2018.
[39]Though see Carnegie and Carson 2018*a*.
[40]Lipson 1984; Mearsheimer 1994.

of theorizing the reasons for information under-provision and uncertainty in international relations.[41] A poor information environment under anarchy is thought to be "one of the central problems confronting countries and one of the main reasons why war persists" and is a "foundational starting point" for classic paradigms like realism.[42] Our focus on adaptation problems offers new insights about why states and firms may be so hesitant to reveal what they know. Moreover, the intelligence and firm-related adaptations we develop are often different than classic sources of uncertainty like incentives to misrepresent military strength and vulnerabilities.[43] Commercial adaptation costs are unrelated to military issues but can deter states from making information available which exonerates themselves. This makes sense of puzzling cases of states withholding information that would exonerate themselves or their allies, examples of which we discuss in Chapter 2. Moreover, the damage from lost intelligence sources and methods is often far afield from direct military vulnerabilities. Our chapter on war crimes, for example, shows how fears of tipping off war criminals can deter disclosures unless a tribunal embraces confidentiality.

1.6.2 Empirical

This book uses a multi-method approach, drawing on original data collection including, among other sources, 64 elite interviews conducted in Geneva, Vienna, New York, and Washington D.C., and archival research from both the security and economic realms. Our archival research sheds light on specific episodes of leaders' intelligence sharing decisions. For example, Chapter 4 presents new evidence from declassified U.S. intelligence material on the timing and precision of American knowledge regarding war crimes by Paul Kagame's forces in Rwanda. The book also presents findings from several data collection efforts. For example, we offer new data on sensitive information and confidentiality features in a sample

[41] E.g., Rathbun 2007.
[42] Mitzen and Schweller 2011, 4.
[43] Fearon 1995.

of 106 international organizations in which we coded IOs with security or economic functions for the presence of information security measures and other related features. One striking finding from this exercise is that such activities are quite common: almost half of the IOs in our sample feature some attempt to integrate sensitive information. We review these data in more detail in Chapter 3.

Additionally, we provide new data and analyses that are related to specific issue areas and are discussed in subsequent chapters on nuclear proliferation, war crimes, trade, and investment. For example, Chapter 6 adds to debates about nuclear weapons development and the causes of non-proliferation using extensive new data on U.S. intelligence sharing with the IAEA – which we gathered primarily from elite interviews, archival material, and other primary sources – as well as new data on nuclear plant closures. This original data allows us to test an under-analyzed mechanism by which the nuclear non-proliferation regime influences countries' nuclear ambitions – via intelligence submissions to the IAEA – which has been identified as "an important next step in research" in this domain.[44] While existing scholarship has largely focused on the role of the broader nonproliferation norm and regime,[45] and the IAEA's role in spreading access to nuclear technology[46] in part due to data constraints, we provide a novel understanding of *how* this institution affects states with clandestine nuclear programs.

Similarly, our new data on intelligence-sharing with the ICTR and ICTY, which was also gathered from a variety of primary and secondary sources, allow us to verify these mechanisms in a very different setting. We demonstrate that international criminal tribunals often rely heavily on the unique insights provided by intelligence to indict and arrest individuals suspected of war crimes. However, the provision of this information is selective, depending on the informed states' political interests, and requires a tribunal with an appropriate confi-

[44]Fuhrmann and Lupu 2016, 538.
[45]Rublee 2009*a*; Coe and Vaynman 2015; Fuhrmann and Lupu 2016.
[46]Fuhrmann 2012; Brown and Kaplow 2014; Brown 2015.

dentiality system. Our findings shed new light on the growing literature about whether IOs are effective in promoting international justice.[47]

In the economic realm, we coded whether sensitive information was provided to or withheld from critical IOs including the WTO and ICSID using novel measures such as redactions in panel reports, mentions of information withholding in panel reports, and other indicators. These original data allow us to contribute to scholarly debates about the WTO and ICSID. For example, past scholarship has argued that the WTO helps to address the temptation to defect from trade agreements,[48] prevents countries from exercising coercive diplomacy,[49] and permits countries to build reputations for trade agreement compliance.[50] A core assumption in most accounts is that the WTO must "verify and publicize violations."[51] Our findings show that secrecy during disputes is essential to accurately diagnose whether a violation has occurred in the first place. Governments may refuse to disclose dispute-relevant information if they fear that their firms will suffer damage. However, the WTO's use of a secure confidentiality system allows sensitive firm-specific details to be integrated and contributes to the more effective adjudication of some kinds of disputes. Finally, new data in Chapter 7 permit us to address a nascent but growing literature on secrecy in foreign direct investment disputes by showing how decreased trust in the confidentiality of investor-state arbitration influenced the kinds of disputes investors and firms pursue.[52]

1.6.3 Normative

Our core findings that IO confidentiality systems can increase states' sharing of sensitive information and thereby improve cooperation may also generate byproducts with potentially

[47] E.g., Sikkink and Kim 2013; Jo and Simmons 2016; Appel 2018.
[48] Bagwell and Staiger 1999.
[49] Carnegie 2014.
[50] Büthe and Milner 2008; Maggi 1999; Mansfield and Pevehouse 2008.
[51] Maggi 1999, 193.
[52] Hafner-Burton, Steinert-Threlkeld and Victor 2016*a*; Pelc 2017.

problematic normative implications. For example, increasing secrecy in IOs may add to the recent criticism of a "democratic deficit" in international institutions that has swelled into a chorus of calls for greater transparency and openness regarding IO activities in international finance, global trade, European integration, and environmental regulation.[53] Advocates argue that transparency can enhance international institutions' accountability and therefore legitimacy.[54] This is especially important for advocates of transnational governance in an era in which international organizations like the European Union are under intense scrutiny and populist scorn even in established Western democracies.[55] In Chapter 7, for example, we analyze the "crisis of legitimacy" that emerged in the realm of foreign direct investment due to popular anger over secretive international arbitration. Increasing secrecy in the manner we describe can thus exacerbate this anger and distrust. In the Yugoslavian war crimes tribunal, for example, efforts to assure intelligence-sharing countries that their sensitive information would be protected through new international legal secrecy measures prompted accusations that such measures create "problems for preserving the openness of international criminal trials."[56]

Yet we identify a countervailing normative benefit as well. Integrating sensitive information can improve the ability of IOs, states, and firms to identify non-compliance, reassuring them that violations will not go undetected. Our empirical chapters show how confidentiality systems in IOs can boost the accuracy of compliance assessments by improving the quality of available information. This, in turn, may enhance the legitimacy of global governance.[57] Indeed, improvements in the confidentiality system at two of the IOs we analyze – the World

[53]Blanton 2007; Ehring 2008; Gupta 2008; Koenig-Archibugi 2004.

[54]Grant and Keohane 2005*a*. However, transparency is not an unalloyed good, as we discuss in later chapters, e.g. Lord 2012.

[55]E.g. Eric A. Posner, "Liberal Internationalism and the Populist Backlash," Public Law Working Paper No. 606, University of Chicago, January 14, 2017.

[56]Moranchek 2006, 479.

[57]However, we discuss possible legitimacy issues that arise due to selective information disclosures subsequently.

Trade Organization and International Atomic Energy Agency – were responsive to critiques of poor monitoring and weak dispute settlement. Ironically, confidentiality systems tend to make an institution itself *less* transparent while rendering compliance behavior *more* transparent, thereby improving cooperation. As we discuss more in Chapter 8, the consequences of confidentiality and secrecy for the normative goals of global governance, and by extension its legitimacy, is an important direction for future research.

1.6.4 Practitioners

Finally, this book has implications for policymakers and IO leaders that confront the tensions and challenges raised by disclosure dilemmas on a regular basis. In Chapter 8, we discuss trade-offs that arise when information is both useful for assessing compliance and dangerous to widely disseminate. This gives some measure of guidance for practitioners in informed states, firms, and those inside IOs that may consider integrating sensitive information. Our claims suggest that innovative approaches to doing so should be of interest to state leaders that hope to improve accountability for war crimes or reduce threats to foreign direct investment.

More broadly, both our theory and empirical findings provide ideas about how and when policymakers have succeeded in integrating sensitive information into broader cooperative efforts, and when this has failed. This includes specific ideas about how complex organizations like IOs can develop and maintain information security in order to elicit disclosures from states or others. This has clear implications for institutional design decisions. We further show how practitioners can capitalize on political opportunities to reform IOs to expand or reduce the use of sensitive information, and we describe the potential political consequences of doing so. Finally, the findings include cautionary notes about how to guard against misunderstandings that result from the inclusion of sensitive information. For example, our theory underscores how IOs can benefit from making their vetting process transparent and

from working hard to elicit disclosures from a diverse range of donors.

1.7 Plan of the Book

Chapter 2 presents our core concepts, develops our theoretical logic, and derives hypotheses for empirical testing. The chapter defines our key terms and discusses the scope conditions on our theory. We then elaborate on what kinds of information are considered sensitive in our framework, and describe the kinds of problems that can arise when such information is necessary for understanding compliance-related questions. We next expand on the necessary features of IOs' confidentiality systems, providing concrete examples. The chapter concludes by developing our two core empirical expectations about the effect of confidentiality systems on the frequency of disclosures of sensitive information and on international cooperation.

In Chapter 3, we provide an overview of sensitive information in global governance and important historical context. The chapter first describes new data on the confidentiality features of a sample of 106 IOs. We review variation in the frequency and form of such protections and show that measures to protect various forms of sensitive information are surprisingly common and vary in interesting ways. It then describes the rise the norm of transparency in diplomacy and global governance after World War I, which then deepened with the end of the Cold War. This is juxtaposed with early examples of IOs experimenting with confidentiality and sensitive information. The chapter concludes by explaining how changes in technology and broader cooperative goals have generally led to efforts to integrate sensitive information into IOs, despite the resulting tension with transparency.

The next four chapters evaluate our claims in four distinct issue areas. Chapter 4 focuses on the realm of nuclear proliferation. Governments with intelligence capabilities often obtain detailed insights into clandestine arms programs including hidden nuclear weapons-related activities. Such sensitive information can bear directly on questions of compliance

with treaties that prohibit the development of new nuclear arsenals. Disclosing such intelligence can facilitate multilateral scrutiny of suspected proliferators but also risks exposing intelligence collection methods, thereby prompting future intelligence targets to avoid detection. We draw on interviews at the IAEA's headquarters, archival research, and newly collected data to assess how an institutional shift toward confidentiality in the early 1990s increased the frequency of the U.S.'s intelligence disclosures about non-allies to the IAEA, and improved the IAEA's ability to monitor their nuclear facilities.

Chapter 5 turns to the domain of international trade, in which governments and firms have incentives to reveal firm-specific details like contracts, profit trends, and supply relationships during the dispute resolution process to help substantiate claims of innocence or document damage from foreign trade discrimination. However, doing so can also expose details that allow rival firms to gain market share or other advantages. We analyze the effects of the WTO's confidentiality improvements surrounding a key case in 2004, the Boeing-Airbus dispute over civil aircraft subsidies. We show that these reforms led to increased submissions of sensitive information using newly collected data on redactions in public-facing WTO reports, requests for confidentiality procedures, and other observable indications of sensitive information disclosures. We also show that these changes boosted trade flows, especially for sectors with greater sensitive information concerns. We pair these quantitative findings with qualitative case studies of four trade disputes at the WTO which demonstrate the conditional importance of sensitive information and the impact of confidentiality reforms.

In Chapter 6 we pivot to the role of national intelligence in the realm of international criminal law and war crimes. Countries with strong intelligence capabilities often encounter unique information that speaks to the guilt or innocence of individual leaders suspected of war crimes. Ad hoc war crimes tribunals, moreover, require detailed evidence to secure indictments, arrest suspected war criminals, and obtain convictions. As with nuclear-related intelligence, disclosing intelligence about war crimes can reveal sensitive sources and methods

which can enable other actors to adapt in ways that jeopardize future intelligence collection abilities. We focus on the behavior of the United States with respect to the International Criminal Tribunal for the former Yugoslavia and the International Criminal Tribunal for Rwanda. Drawing on newly reviewed archival materials, elite interviews, and secondary sources, we find that the inclusion of confidentiality systems in the tribunals elicited greater intelligence disclosures for leaders who did not have strong geopolitical relationships with Washington. Intelligence implicating Slobodan Milosevic, for example, was withheld until a confidentiality system was put in place and his role in peace-related diplomacy ended. Disclosed intelligence, in turn, played an important role in obtaining indictments and facilitated the arrests of key war criminals.

Our attention in Chapter 7 shifts to foreign direct investment, which allows us to apply our framework to a context in which a non-state actors (investors, typically firms) directly participate and where confidentiality assurances have declined rather than expanded. Access to sensitive information from firms and host governments can be essential for assessing whether a state has violated its FDI related agreements. However, sensitive materials from host governments can raise political sensitivities, and the disclosure of detailed project-specific information can prompt harmful commercial adaptations that erode firms' market shares. We focus on the International Centre for Settlement of Investment Disputes (ICSID), an IO that arbitrates claims of investment violations between firms and governments. Rather than improving the integration of sensitive information, changes to investor-state dispute transparency rules have relaxed the tradition of secrecy in arbitration at ICSID. Drawing on interviews and newly collected data, this chapter demonstrates that this increased transparency has deterred the pursuit of arbitration by firms and states, and dampened FDI flows in risky and non-transparent countries.

We conclude in Chapter 8 by discussing the argument's downstream implications and its scholarly, practical, and normative contributions. We first return to the themes of trans-

parency and power, assessing our empirical findings and related literatures. We analyze how the presence of a confidentiality function in an IO may influence power dynamics and institutional transparency and derive implications for understanding how IOs can manage such tensions. We also synthesize lessons from existing research on path dependence as well as findings from our four empirical chapters to reflect on the likely origins and decline of confidentiality systems. The chapter then discusses the broad relevance of our theory for other empirical domains, briefly reviewing extensions to peacekeeping, international finance, cybersecurity, and environmental issues, which suggest the wide applicability of our framework. We conclude by analyzing the implications of our claims for scholarship on international politics.