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 were 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 and allowed 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 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

[1] Branigin, William. "U.S. Evidence Enhances Case against Milosevic." *Washington Post*, May 28, 1999; Manning 2000, 1, 12, 16.
[2] Scheffer 2012, 274.
[3] Marise Simons. "U.S. and Britain Vow to Give War Court Data on Top Yugoslavs." *New York Times*, April 18, 1999.

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 Milošević.[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 international organizations (IOs) might integrate it, and the effects of such efforts. Such a lack of knowledge is particularly striking in view of 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-quality information to monitor a ceasefire without revealing a government's sources?

Secrets in Global Governance sheds light on these issues. In doing so, it addresses two central research questions. First, what factors induce states and firms to disclose their sensitive information to address questions of compliance? Second, what impact does sensitive information have on the effectiveness of IOs and the cooperative goals they are designed to further? Our answers address several long-standing debates in the study of international relations: these include the barriers to cooperation that states face under anarchy, how formal IOs mitigate such barriers, and the sources of power and uncertainty in

[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.

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 placed under severe duress. This book suggests ways to make IOs more effective and responsive by providing insights into how they work and how information circulates within them.

To do so, we disaggregate "information" into two types: sensitive and nonsensitive. Sensitive information refers to private information whose wide dissemination would allow changes in the behaviors of other state and nonstate actors that are harmful to the discloser. We assess 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

[8] Keohane 1984.

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, increase the potential 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 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

[9] For example, Grigorescu 2003, 2007, 2015; Koppell 2010; Tallberg, Sommerer and Squatrito 2013; Tallberg et al. 2014.

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 the potential assumption of incrimination benefits to affect the frequency of sensitive information disclosures. We then show how this information provision can have an impact on the success of efforts to cooperate. The result is a novel story about how equipping IOs with secrecy can allow the international community to harness the unique but sensitive insights of both states and firms.

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 nonstate 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, thus 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 both "as a repository and communicator of information."[13]

[10] Mitchell 1998; Dai 2002.
[11] Mansfield, Milner and Rosendorff 2002; Dai 2002, 2005; Thompson 2006; Chapman 2007; Fang 2008.
[12] Keohane 1984, 94.
[13] Dai 2002, 411.

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 "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 on 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 (IMF) developed a three-tiered classification system for highly sensitive banking-related documents to

[14] Colson 2008.
[15] Grigorescu 2007, 625.
[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.

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 IOs 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 International Atomic Energy Agency (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 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]

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

however, such information can be difficult to obtain. Detecting noncompliance often requires specialized techniques or knowledge that only specific states or nonstate 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 investments. Alternatively, sensitive information might substantiate claims of a competitor or rival's wrongdoing. 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 nonstate 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

[23] Hafner-Burton 2008.

[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."

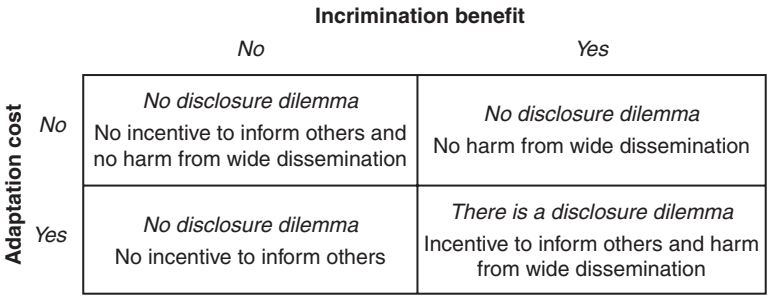

Figure 1.1 Conditions for disclosure dilemmas.

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 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 not only reduce adaptation costs but also reduce the benefits by creating credibility problems.

1.3 The Solution: IOs and Sensitive Information

We argue that IOs, 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 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] IOs 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.

[25] Geser 1992; Gibson 2014.
[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; Chapman 2007.