H-Diplo | Robert Jervis International Security Studies Forum

Roundtable Review 15-52


12 July 2024 | PDF: https://issforum.org/to/jrt15-52 | Website: rjissf.org | Twitter: @HDiplo

Editor: Diane Labrosse  
Commissioning Editor: Matthew Fuhrmann

Production Editor: Christopher Ball  
Pre-Production Copy Editor: Bethany Keenan

Contents

Introduction by Matthew Fuhrmann, Texas A&M University ................................................................. 2

Review by Natalie Bryce, UCLA, and Leslie Johns, UCLA ................................................................. 6

Review by Melinda Haas, University of Pittsburgh GSPIA ................................................................. 10

Response by Allison Carnegie, Columbia University, and Austin Carson, University of Chicago .14
What is the role of secrecy in international relations? Does secrecy promote or stymie cooperation among countries? And what role do international organizations (IOs) play in this context? Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation by Allison Carnegie and Austin Carson takes on these questions, which are critical for both academic research and public policy. It presents a novel argument: international organizations can facilitate cooperation when they are better equipped to keep sensitive information confidential. This challenges the conventional wisdom, popularized by political scientists in the 1980s, that international organizations promote cooperation by sharing information and bolstering transparency.\(^1\) The book develops and tests this argument in several contexts: nuclear proliferation, international trade, war crimes, and foreign direct investment. It deliberately chooses IOs that function in three different areas—security, economics, and humanitarian issues—thereby showing the scope and breadth of the book’s arguments.

In this roundtable, both reviews zero in on the book’s central conundrum: when should countries share sensitive information with IOs? Doing so can greatly enhance the efficacy of the IO, providing an incentive to share information freely. However, if the IO is unable to keep shared information confidential, it can also harm a state’s interests by revealing its sources and methods, which is a central challenge in the world of intelligence. Solving this dilemma is crucial for helping IOs function effectively, and Carnegie and Carson convincingly document how this can be done. As Melinda Haas writes, they have produced the “definitive work” for how IOs can use secrecy to enhance compliance.

Recent events, particularly Russia’s invasion of Ukraine in February 2022, have underscored the salience of Secrets in Global Governance, a point that is underscored by Haas. The United States has shared intelligence at critical junctures during this conflict, sometimes directly with the public and on other occasions with IOs such as the International Criminal Court (ICC). The book helps us better understand why this has happened, and when sharing information with IOs can backfire. The International Atomic Energy Agency’s (IAEA) role in this conflict—particularly when it comes to safeguarding the Zaporizhzhia nuclear power plant—also underscores the key role that IOs can play in providing credible information to the public during the “fog of war,” which itself can have a deterrent effect on military attacks.

The two reviews highlight some of the key implications of the book and point to directions for future research. Great books often push readers to consider extensions and counterarguments, and that is the case here.

Natalie Bryce and Leslie Johns usefully focus on the book’s implications for war crimes. They raise an interesting possibility: access to information on war crimes gives leaders power, allowing them to facilitate

---

the prosecution of their domestic rivals—especially in authoritarian regimes. To illustrate this point, they highlight Uganda’s sharing of information with the ICC to aid in the prosecution of a rebel in the Lord’s Resistance Army. Bryce and Johns then tease out two of the book’s assumptions. One is that IOs primarily rely on states to obtain information. However, they point out that IOs themselves can collect information too, even if states do not voluntarily share it. A second assumption is that states usually convey truthful information to IOs. But Bryce and Johns ask a thought-provoking question: what if states lie in order to gain an advantage?

Haas similarly raises interesting questions about the book. She asks whether countries might be better off disclosing information independently, rather than sharing it with IOs. Haas also wonders about how much agency IOs have. Do they have their own identity or do they merely reflect the interests of individual states? She further points out that it can be difficult for IOs to seek out the information they need to ensure compliance, especially in the security arena, due to concerns about state sovereignty. IOs therefore need to be seen as legitimate in order to serve their information-collecting functions—for example, in the way the IAEA inspects a country’s civilian nuclear facilities to ensure that materials have not been diverted to a nuclear weapons program. Finally, Haas interestingly comments on how process transparency can be important for legitimacy, even if IOs (or other actors) do not share sensitive information.

In their response, Carnegie and Carson constructively engage with these ideas. They explain why they roped-off domestic politics in the disclosing state when building their theory, while also highlighting that this represents a compelling avenue for future research. Carnegie and Carson also consider sources of information sharing beyond states. They acknowledge that information from non-state sources can be valuable to IOs. At the same time, they underscore that information from states is particularly valuable because it is more accurate and precise. On top of this, states intentionally constrain the information-gathering capabilities of IOs in order to protect their sovereignty. Carnegie and Carson agree with Bryce and Johns’s point that states can share false information so as to gain an advantage. This is why, Carnegie and Carson argue, IOs are important: they do not usually accept information from states at face value, instead subjecting claims to scrutiny to get to the truth. States anticipate this possibility and are therefore often deterred from lying.

Carnegie and Carson further clarify why states might prefer to share information with an IO instead of just revealing it themselves. By acting alone, a state might gain some diplomatic and political advantages but compromise its sources and methods. The existence of a relevant IO opens the possibility that a state can reap the benefits of information sharing while dodging some of the costs—if the IO can maintain confidentiality. Carnegie and Carson also acknowledge the importance of IO agency. They argue that in many cases IOs have preferences that are independent of states; this is important for assessing information and getting to an objective truth. They also highlight the ways in which studying how different forms of transparency—including procedural transparency—could move the literature forward.

This roundtable underscores three things. First, the study of secrecy in the context of IOs is both interesting and important. Second, Carnegie and Carson’s book represents a big leap forward towards better
understanding this issue. Third, some questions remain unanswered and there are interesting avenues for future research.

Contributors:

Allison Carnegie is a Professor of Political Science at Columbia University. She received a joint PhD in political science and economics from Yale University in 2014. Her research interests include international relations, international organizations, and international political economy. In addition to Secrets in Global Governance, she is the author of Power Plays: How International Institutions Reshape Coercive Diplomacy (Cambridge University Press, 2015), Perils of Populism: How Populism is Warping Global Governance (in progress), as well as a variety of academic and policy pieces.

Austin Carson is an Associate Professor of Political Science at the University of Chicago. His research addresses the role of secrecy and intelligence in international relations theory, international conflict, and global governance. In addition to Secrets in Global Governance, he is the author of Secret Wars: Covert Conflict in International Politics (Princeton University Press, 2018). He has published articles in International Organization, American Journal of Political Science, Security Studies, and other venues. His books and articles have won numerous awards including the Lepgold Prize for Book of the Year, the Robert O. Keohane Award, ISA’s Best Security Article Award, and the Best Book Award from APSA’s International Collaboration section. He received his PhD from Ohio State University in 2013.


Natalie Bryce is a PhD student in the UCLA Department of Political Science. Her scholarship focuses on international law, human rights, political violence, and international organizations. Broadly, her work explores how international politics influence the prevention and punishment of international crimes.

Melinda Haas is Assistant Professor of International Affairs at the Graduate School of Public and International Affairs at the University of Pittsburgh. Her research addresses the how congressional oversight regulation can have unintended effects on the types of covert action used in US foreign policy.
Her other research interests include foreign policy decisionmaking, intelligence and secrecy, as well as international and constitutional law. Her research is published in *International Security*, the *International Journal of Intelligence and CounterIntelligence*, and *The Diplomat*.

**Leslie Johns** is a Professor of Political Science and Law at UCLA. Her research focuses on international law, organizations, and political economy. She is the author of *Politics and International Law: Making, Breaking, and Upholding Global Rules* (Cambridge University Press, 2022) and *Strengthening International Courts: The Hidden Costs of Legalization* (University of Michigan Press, 2015). Her articles have appeared in peer-reviewed journals such as the *American Political Science Review*, *International Organization*, and *The Journal of Politics*. She received the Michael Wallerstein Award for political economy in 2017 and has held multiple fellowships at Princeton University.
“Secrecy, Information, and Power in International Criminal Tribunals”

As early as May 1994, the US State Department had concerns about atrocities committed by Rwandan Patriotic Front Commander Paul Kagame and his troops during the Rwandan genocide (chapter 6, footnotes 167-169). US intelligence had incriminating satellite images, radio signals, and information about the whereabouts of suspected criminals serving in Kagame’s forces. Yet the US government chose not to share this information with the International Criminal Tribunal for Rwanda (ICTR), which was created by the UN Security Council to prosecute serious international crimes, including those against humanity, genocide, and war crimes, that took place in Rwanda in 1994.1

In their book, Allison Carnegie and Austin Carson describe how states face disclosure dilemmas when deciding whether to share this type of sensitive information with international organizations (IOs). Sharing information can create incrimination benefits for states by increasing international cooperation and helping states to achieve their political goals. However, sharing information can also create adaptation costs, such as the exposure of confidential sources and methods. Carnegie and Carson argue that states are more likely to reveal their secret information—thereby overcoming their disclosure dilemmas—when an IO has a confidentiality system that allows it to keep sensitive information private. Yet confidentiality systems are not a cure-all. While states may share secrets that implicate their enemies, they will still hide information that incriminates their allies.

Carnegie and Carson support their argument using detailed case studies of the International Criminal Tribunal for the Former Yugoslavia (ICTY) and the ICTR. As the first international criminal tribunal created since World War II, the ICTY was a major legal innovation and experiment. The ICTY initially did not include strict confidentiality procedures because of concerns about due process. Carnegie and Carson argue that the US accordingly refused to share valuable intelligence about perpetrators because it feared that the ICTY would reveal information about intelligence sources and methods. States subsequently reformed the ICTY’s confidentiality policies, prompting the US to provide a trove of fresh intelligence that helped the ICTY to increase convictions of high-level suspects (chapter 6, pages 227-228). These reforms were then implemented at the ICTR (chapter 6, page 241). These case studies illustrate Carnegie and Carson’s argument that if proper confidentiality policies are in place, international criminal tribunals will receive more tips from states and thus will be more likely to conduct successful prosecutions.

The authors also analyze how the US selectively provided and withheld evidence to both tribunals based on whether crimes were committed by perceived international allies or enemies. When political conditions changed, for example, when former president of Serbia Slobodan Milošević was no longer perceived as a

1 Specifically, the ICTR was granted jurisdiction to prosecute crimes against humanity, genocide, and violations of Article 3 Common to the Geneva Conventions and of Additional Protocol II committed in the territory of Rwanda or by Rwandan citizens in neighboring states.
trustworthy ally in international peace negotiations, so too did US strategy for cooperating with the ICTY. At the ICTR, the US only provided evidence against defendants from the former Habyarimana regime. In contrast, the alleged crimes of US ally Paul Kagame and his troops were systematically overlooked. Carnegie and Carson thus illustrate that even when disclosure dilemmas are overcome, states will only share information if doing so aligns with their political interests.

While Carnegie and Carson focus on the Yugoslavia and Rwanda tribunals, their arguments can be applied to all international criminal tribunals (ICTs). The full set of ICTs includes the International Criminal Court (ICC), which is a permanent institution with 123 member-states. ICTs also include numerous mixed criminal tribunals, which prosecute individuals using a blend of domestic and international law, personnel, and/or procedures, such as the Special Court for Sierra Leone. Given the broad scope of Carnegie and Carson’s argument, we wish to highlight one major implication and two key assumptions of their work. These points are important for the application and generalizability of Carnegie and Carson’s claims about secrecy, information, and power in international criminal tribunals.

First, an important implication of Carnegie and Carson’s argument is that information about serious international crimes is inherently a form of political power that can be used to challenge international rivals and protect international allies, as shown by the examples of Milošević and Kagame. Yet Carnegie and Carson’s argument can be pushed further; information about serious international crimes can also allow leaders to use ICTs as tools for confronting domestic political rivals. Dictators have particularly strong incentives to adopt these tactics when they face strong political competition. Additionally, dictators control the military and police agencies that collect information needed by international prosecutors who are without administrative and judicial restrictions that might limit disclosure. In contrast, domestic political opponents who challenge sitting dictators will not have the same access to information about crimes committed by governments.

This pattern is apparent in the ICC trial of Dominic Ongwen, a mid-level commander in the Lord’s Resistance Army (LRA), a rebel group in Uganda. In Ongwen’s trial, the ICC Prosecutor relied extensively on recordings and logbooks of LRA radio communications. These communications were intercepted, screened, recorded, and translated by the Ugandan military and intelligence agency, as well as by local police forces. The Ugandan government then provided edited recordings and selected logbook entries to ICC investigators, who used these materials as evidence against Ongwen. In contrast, the LRA lacked the capacity to collect evidence about the activities and communications of the Ugandan military. Just as the

---


US used its superior intelligence capabilities to punish its international opponents and reward its allies at the ICTY and ICTR, Yoweri Museveni, the incumbent President of Uganda, used his absolute control over the Ugandan military and intelligence services to punish his domestic political opponents at the ICC.

Second, an important assumption is that international prosecutors cannot collect information themselves. They rely on states to provide evidence that is necessary for a successful prosecution. However, international organizations often collect sensitive information independently of states. For example, the UN Human Rights Council has increasingly created fact-finding inquiries to investigate alleged violations of international law. The evidence collected by these inquiries may then be used in later international criminal prosecutions. For instance, the ICC has used inquiry reports for criminal prosecutions involving individuals from Côte d’Ivoire, Guinea, Kenya, Libya, and Sudan. Non-governmental organizations (NGOs) also collect and provide information to international criminal tribunals. Human Rights Watch led a major campaign to collect evidence and push for the prosecution of former Chadian dictator Hissène Habré. The group spent 15 years and millions of dollars gathering documentary evidence and witness testimony, lobbying governments, and helping to craft the legal strategy that ultimately culminated in Habré’s trial at the Extraordinary African Chambers, a mixed criminal tribunal that was created by the African Union and Senegal specifically to prosecute Habré. Similarly, NGOs can file complaints and request consultations with the ICC’s Office of the Prosecutor. These documents and meetings often form the basis for the ICC’s preliminary examinations, like the ICC’s recent operations in Nigeria, Palestine, the Philippines, and Ukraine. Observers have even credited the eventual opening of a formal investigation in Palestine to the concerted efforts of a coalition of NGOs.

Third, another important assumption is that states always truthfully reveal their private information. That is, Carnegie and Carson do not consider the possibility that states might knowingly provide false evidence to a criminal prosecutor, thereby resulting in a false prosecution or conviction. For example, several states have recently been credibly accused of abusing the Interpol Red Notice system. When states experience

---


regime change or civil war, opponents of the regime may flee in order to avoid being subject to dubious justice systems in their home state. Similarly, members of the regime who find themselves on the wrong side of a dictator or who have a change of heart often try to escape to democracies where they can seek asylum. In these situations, home states may try to locate and arrest these individuals by filing an Interpol Red Notice, which functions as a request for law enforcement authorities worldwide to locate and arrest a wanted individual pending extradition. Prosecutors in the states that host these wanted refugees often have no way to verify whether these requests are genuine or whether they are an attempt to target political opponents. Many notable examples have come to light in recent years in which dictatorships have been discovered filing false information with law enforcement authorities to try to extradite political opponents. States that have been credibly accused of abusing the Interpol Red Notice system include Algeria, Azerbaijan, Bolivia, China, Egypt, India, Iran, Kazakhstan, Russia, Tajikistan, Turkey, Ukraine, and Uzbekistan.

In 1994, the US chose not to disclose secrets that could incriminate Kagame and his troops. Carnegie and Carson’s book highlights the importance of this kind of strategic information sharing for international criminal tribunals. Yet choosing to withhold information is not the only choice available to states – they can also allow investigators selective access to information in order to target domestic political opponents or share false information to ensure that these opponents are extradited back to the state’s realm of control. However, international organizations and NGOs can counterbalance these activities by conducting their own investigations and working to thoroughly verify intelligence provided by states. Indeed, our present understanding of the actions of Kagame and his supporters is in many ways due to the documentation efforts of these groups. As Carnegie and Carson rightly point out, secrets, information, and power are key determinants of who faces justice in international criminal tribunals.

---


Review by Melinda Haas, University of Pittsburgh GSPIA

Allison Carnegie and Austin Carson’s *Secrets in Global Governance* does more than just extend the growing literature on the importance of secrecy in international relations, it is the definitive work on how international organizations (IOs) can use secrecy to enhance compliance. The authors use qualitative and quantitative evidence to show how the introduction by IOs of confidentiality mechanisms for sensitive state information increases information disclosure and therefore improves the functioning of those IOs. In particular, the numerous case studies, interviews, and careful descriptive analysis of the onset of the confidentiality mechanism in IOs make it clear that the trends they identify are not epiphenomenal or limited to certain issue areas, and that they are an effective way to increase the abilities of IOs to police compliance.

Carson and Carnegie add nuance to their explanation in order to apply across economic and security domains. In particular, despite the IOs’ confidentiality systems, states make choices as to whether to share intelligence information based on geopolitics. The authors find that despite the existence of the confidentiality systems, states are unlikely to share information that implicates their allies in bad acts. This relates to the book’s strong theoretical arguments regarding states’ utility calculations when faced with a disclosure dilemma—namely, incrimination benefits and adaptation costs.

My personal research interests lead me to push on the book’s relevance to intelligence disclosure writ broadly. The book focuses its theory to the disclosure of compliance-related information to IOs, but the authors’ argument has implications for the broader literature on public intelligence disclosure. For example, intelligence disclosures to an IO may assist in preventing, prosecuting, or punishing war crimes, as chapter 6 attests. But why would a state choose to share this type of information with an IO rather than publicly disclose it themselves? If the information is kept secret by the IO, then no sources and methods, or adaption costs, will be risked. Intelligence disclosure during the course of the IO’s actions may however create similar risks to expose national capabilities. What does an IO provide in this case, other than a means of laundering its intelligence assessments without the disclosure of the sources and methods? This argument is similar to Alexander Thompson’s *Channels of Power* and how IOs, namely the UN Security

---


Council, can launder states’ arguments and legitimize intervention through strategic information transmission to foreign leaders and their publics.¹

This point about IO function leads me to another question on IO identity. Although the authors ably describe how confidentiality mechanisms can encourage disclosure, I would like to see more delineation of how IOs function in the author’s theory. Are they simply functional aggregators for compliance information (even if not conveyor belts of such), or are they institutions with their own identity that is separate from the loci of power within them?² Carnegie and Carson discuss how much of international relations literature sees IOs as a tool to ease access to compliance information,³ but they also argue that IOs can develop cultures that reward secrecy, which can bolster a reputation for trustworthiness with sensitive information.

But not all IOs that address compliance-related questions are created equal. As the authors remind us, military information on a state’s vulnerabilities may be sensitive but is outside the scope of their argument unless that information bears on international rule compliance issues. Although the International Atomic Energy Agency (IAEA) and the International Criminal Court (ICC) are both security institutions, I would argue that they are good at encouraging intelligence disclosure because both are seen as having the legitimacy to intrude into other states’ sovereignty in ways that other states could not do unilaterally. There is a sweet spot of using states’ intelligence disclosures to enforce compliance without overstepping. This is why states disfavor empowering an IO to collect sensitive information itself; they do so in order to prevent such slippage and violations of informational sovereignty. This slippage is a particular risk under questions of compliance with rules regarding the use of force, as many issues of international humanitarian law lack clear answers that can be enforced without controversy.

Chapter 3 addresses the question of why, if transparency is a highly valued norm, especially in global governance, IOs are empowered with confidentiality. Related to my comments on theorizing on the agency of IOs, do IOs serve to push transparency norms through entrepreneurship? Or do they reflect the opinions of the states that make them up? Given Rachel Myrick’s findings that transparency norms are less

---


important to US domestic publics than ensuring favored foreign policy outcomes, perhaps there is still some cheap talk remaining in the value placed on transparency over ensuring compliance outcomes.  

Similarly, the dissonance between instituting confidentiality systems and bolstering institutional transparency may be resolvable. Although some audiences may be excluded—namely other member-states or outsiders—it is possible to permit intervention by other interested parties. The ICC provides opportunities for victims to file applications of participation and reparations in connection with war crimes prosecutions. Even more importantly, we can distinguish the value of transparency in process versus substance. Inclusive, transparent procedures may be more important in creating legitimate IOs than requiring transparency as to the substance of the disclosed information. Again referring to the domestic context, US law provides for review of classified information only by the judge presiding over the litigation and without submission to other parties. When process transparency is lacking, as is the muddled role of secrecy in the war crimes trials at Guantanamo Bay, those compliance-based decisions lack legitimacy. Thus, it is not only the existence of confidentiality systems, but also the means of employing secret information in legitimate enforcement of compliance, that is crucial to empowering greater cooperation within IOs.

The book’s impact can already be seen in how it has inspired follow-on literature. For example, scholars have expanded on the dynamics of public intelligence disclosure, particularly as it has been used in the Russian invasion of Ukraine. The authors mention that one way of avoiding adaptation costs is through disclosing sensitive information only to trusted and friendly parties. As we see in the case of Ukraine, the Biden administration used intelligence disclosure to European allies to convince them of the impending Russian invasion. Carnegie and Carson’s extension of secrecy to domains beyond security has also encouraged scholarship on secret negotiations in economic, diplomatic, and intrastate conflicts. I look
forward to seeing how this book revolutionizes the next wave of secrecy scholarship, as well as new avenues in the study of international organizations and compliance.

Response by Allison Carnegie, Columbia University, and Austin Carson, University of Chicago

We would like to first thank Matthew Fuhrmann for putting together and introducing this roundtable on our book *Secrets in Global Governance*, and for his insightful and thought-provoking introduction. We have long enjoyed reading H-Diplo roundtables and it is an honor to be a part of one. We are also very appreciative of Leslie Johns, Natalie Bryce, and Melinda Haas for their thoughtful contributions.

One goal we had in writing *Secrets in Global Governance* was to apply our concepts and theoretical claims broadly with chapters that cover security, economic, and humanitarian issues. We found the recurring role of confidentiality and different kinds of sensitive information in international organizations (IOs) striking. From the beginning, our hunch was that this was an underexplored feature of multilateral cooperation with important stakes. Russia’s invasion of Ukraine in February 2022 underscored those stakes. Media reporting in the last two years has detailed how the United States shared sensitive intelligence with the International Criminal Court about Russian war crimes and troubling concerns about the ICC’s ability to keep such sensitive disclosures secret.¹

The review from Bryce and Johns focuses on one domain that we address: international criminal tribunals (ICTs). As they note, *Secrets in Global Governance* makes the case that state-disclosed intelligence material can provide unique and powerful evidence of war crimes that is not available from other sources. Beyond this domain, the book also explores how confidentiality and sensitive disclosure work in another issue area involving intelligence (nuclear proliferation) and two private-sector issue areas (trade disputes and foreign investment).

Regarding war crimes, Bryce and Johns’s review first builds on our idea that information and disclosure are a form of power. They usefully highlight a domestic version of this dynamic: Leaders who have access to military and intelligence information can selectively reveal or withhold information that is supplied to regional or global governance institutions in order to discredit or punish domestic political opponents.

This idea is a valuable extension of our framework that has much promise for future research. Our theoretical model in *Secrets in Global Governance* intentionally brackets the domestic politics of the disclosing state. This theoretical simplification allowed us to analyze the rich, complex, and normatively significant interstate dynamics. But we agree with Bryce and Johns’s point that unequal access to sensitive information exists domestically as well as among states. Incumbent leaders have more of it than rebel groups. One important implication of their extension, moreover, is that global governance may unintentionally disadvantage rebel groups. The more important disclosed intelligence becomes to multilateral

organizations, the more incumbent leaders should be able to withhold or disclose intelligence in order to bolster their domestic power.

A second point made by Bryce and Johns usefully highlights how sensitive information from states is only one source of information. International organizations, they rightfully point out, may ferret out information on their own or solicit it from non-state actors. The intelligence and corporate information we focus on in the book—which is shared by governments—is not the only game in town.

Our theory and empirical analysis feature three points about other sources of information. First, we argue that sensitive information from states is often uniquely valuable for documenting non-compliance with international laws and norms. Fact-finding missions and studies by non-governmental organizations (NGOs) are useful, but typically do not have the precision and evidentiary power of intelligence. Satellite imagery of North Korea from consecutive days, for example, can show active efforts to hide sensitive nuclear facilities. No other source of information could reliably document a sequence of actions in a closed political environment like North Korea. Second, we argue that the limited quality of information that IOs can gather on their own is no accident. Member-states decide what IOs can and cannot do. States intentionally limit the information-collection powers of IOs in order to retain political control and protect sovereignty. Third, other sources of information do play a key role in helping IOs assess sensitive disclosures by states. Triangulating among different information sources is one way in which IOs vet the accuracy of sensitive disclosures and make a broad case for, say, the guilt of a war criminal.

One promising direction for future research is a more careful comparative study of information from international organizations, states, and NGOs. Some of the examples Bryce and Johns mention hint at how the quality of information from non-state sources is evolving. Groups like Human Rights Watch may learn new techniques for gathering testimony or documenting atrocities from previous conflicts and campaigns. The Human Rights Council staff may help push for more effective fact-finding inquiries. In the book, we find some signs of this in chapter 4, where we show that the International Atomic Energy Agency is not a passive recipient of intelligence and that it actively lobbied member-states for sensitive information. Entrepreneurship by the IO can be one reason for the kinds of confidentiality reforms that we show produce important changes.

In their final point, Bryce and Johns raise an important issue: lying, especially untruthful disclosures by dictators. Bryce and Johns rightly highlight that disclosure procedures and confidentiality mechanisms are available to a wide range of governments. We agree and argue in the book that the possibility of false information is why IOs matter. This is one feature that distinguishes disclosures to an IO from disclosure publicly—a point we return to below when addressing Haas’s review. When states publicly reveal sensitive information, no IO is checking their work. States are free to distort facts for political reasons. Submitting those same details to an IO, which is staffed by subject-matter experts and tasked with finding the truth about rule-breaking, provides a check on untruthful disclosures.
This logic implies that if IOs are equipped with confidentiality measures, most false disclosures that states could make will never actually be made. The likelihood of being caught in a lie by a judge in a war crimes trial or an inspector of nuclear compliance deters it. That said, Bryce and Johns helpfully identify examples of false disclosures to Interpol that were designed to enable dictators to engage in political reprisals. The key question, from the perspective of our arguments in *Secrets in Global Governance*, is what happens after these claims are made. Does the government disclose a dossier of evidence that supports Red Notices? If little evidence follows such claims, our book’s arguments suggest that such efforts will have little meaningful impact. And this is by design.

Haas also raises questions about the added value of disclosure to global governance institutions versus public disclosure. She raises the possibility that IOs are simply laundering the intelligence of states. In the extreme, an IO could receive intelligence and simply put the information and conclusions on its own letterhead. In raising this point, Haas usefully draws attention to recent research on the strategic value that states see in publicly disclosing intelligence, as the United States recently did in the run-up to Russia’s invasion of Ukraine.

We think the comparison to public disclosure is critical and helps illuminate some of the more important claims in the book. States can gain unique public relations and diplomatic advantages from disclosing intelligence publicly. Yet our theory notes that this comes at a steep cost. If public disclosure is the only option, states and private firms are often deterred from doing so by the political and commercial cost of public revelation.

This is the essence of the “disclosure dilemma” that we argue IOs help address. With no IO option, states face a stark choice. They may withhold sensitive details from their public claims, but this sacrifices the credibility and thus potency of going public. A state that provides detailed evidence in public, however, risks what we call “adaptation costs,” such as other intelligence targets learning how surveillance is done and evading it in the future (the “sources and methods” problem). The purpose of empowering IOs to receive and vet intelligence is to give a third option. The added value of IOs is to allow states to use intelligence while minimizing adaptation costs. IOs can do so successfully, we argue, if an effective confidentiality system exists.

Haas also asks how much agency international organizations have in this process. Do IOs and their staff have separate preferences from states? Is the role of an IO to simply aggregate insights from intelligence or other sources? These are important questions. While states and their political goals are front-and-center in *Secrets in Global Governance*, our theory does require that IOs have different preferences than the disclosing state and have agency when vetting disclosed information; otherwise, their assertions lack credibility. We argue that IOs must be proactive in investigating whether disclosures are truthful and in finding new information that is based on accurate disclosures. The career incentives of staff and organizational incentives of IOs drive this process. This is not always the case; for example, we discuss how UNSCOM was co-opted by the U.S. and lost credibility as a result. However, we find that it holds for many important IOs that we describe.
Finally, Haas raises the idea that the dissonance between creating confidentiality systems and bolstering transparency could be resolved with “process transparency.” We agree that this is a potential workaround and explore similar ideas in the conclusion of the book. As her examples suggest, there are important ways in which secretly disclosed information can coexist alongside transparency in the process an IO uses to reach judgments and justify those conclusions. Yet we do think it is important to acknowledge that there may be some upper limits to such efforts. As we discuss in Secrets in Global Governance, some state and non-state audiences will see reasons for questioning conclusions in which sensitive details are not publicly visible. We think that the comparative efficacy of different transparency and confidentiality features remains a fascinating direction for future work.

One goal in writing Secrets in Global Governance was to inject a new perspective on the way cooperation works in practice. Sensitive information and secrecy that protects it do not have a large role in prior scholarship on international cooperation and multilateralism. We hope that the book productively provokes thought and research about the purpose of such practices. As both of these reviews point out, there is still much to learn about the role of secrecy in global governance. We greatly appreciate these insightful reviews and hope that this discussion can help push this research agenda forward.

---