Carnegie, Allison, and Austin Carson. 2023. "Scared to Share: Why Fighting Pandemics Requires Secrecy, Not Transparency." *Global Perspectives* 4 (1). https://doi.org/10.1525/gp.2023.57639.

Political Economy, Markets, and Institutions

Scared to Share: Why Fighting Pandemics Requires Secrecy, Not Transparency

Allison Carnegie[1] [a], Austin Carson[2] [b]

[1] Columbia University, New York, NY, US, [2] University of Chicago, Chicago, IL, US

Keywords: Information, Secrecy, Covid-19, World Health Organization, Confidentiality, Multilateralism

https://doi.org/10.1525/gp.2023.57639

Global Perspectives

Vol. 4, Issue 1, 2023

This article analyzes how fears regarding information disclosure have shaped responses to the COVID-19 pandemic and whether innovations in confidentiality at institutions like the World Health Organization may address those concerns. Sensitive information abounds in global health crises including health data, treatment options, and treatment administration. This creates a dilemma: sharing information is necessary to identify outbreaks but is prevented by concerns regarding privacy, profits, and political scrutiny. Building on insights from other institutions and issue areas, we assess how global governance institutions might respond to these disclosure dilemmas by developing forms of confidentiality in global disease governance. We analyze the benefits and trade-offs in equipping organizations like the World Health Organization with stronger methods for keeping sensitive information secure. We also use new data on a range of international organizations to show that such enhanced confidentiality can improve institutional effectiveness.

The COVID-19 global pandemic has disrupted economies, undermined national governments, and cast a harsh light on global health governance. What is the future of multilateralism for institutions like the World Health Organization (WHO) and for threats like contagious diseases? Building on our research on how fear limits critical information disclosures about other transnational challenges, this article develops reasons why new secrecy capabilities in multilateral institutions may be an important way to better address future disease outbreaks.

Ignorance that results from states and other actors withholding information allows disease outbreaks to multiply and expand. Epidemiologists and the WHO have long recognized this. Indeed, the WHO's most important goals are informational, from building states' capacities to monitor illness in their populations to facilitating early reporting and issuing public declarations of emergency. Information sharing helps in all phases of disease response: identifying outbreaks, containing their spread, and finding effective treatments and vaccines.

Yet the global response to the COVID-19 outbreak was a case study in slow information sharing and even misinformation. Refusals to disclose data and information were perhaps most glaring in the early phases of the outbreak. China appears to have waited weeks to report key milestones in the disease's early spread. The WHO was criticized for dithering in labeling COVID-19 a public health emergency and later a global pandemic. As countries and the world adapted and vaccines were rolled out, the United States, China, and others waged public relations battles via jarringly different narratives about the origins of the outbreak. The transition to vaccine distribution demonstrated anew the dangers of poor information sharing. Addressing all aspects of future disease outbreaks requires overcoming this central challenge.

It is ironic that information-related failures have encouraged the spread and hindered the response to COVID-19, given the current environment of seemingly ubiquitous data, inescapable social media, and crowdsourced internet sleuthing. Far from suffering from an information overload, however, the international community has had to confront a deadly reluctance to share critical data and documents about communicable diseases. Unfortunately, state and non-state actors continue to balk at the costs of surrendering key data and details. Cooperating on these kinds of global challenges is not simply a question of having clear rules and shared interests. Despite the substantial health benefits from sharing information related to the pandemic, individuals, firms, and states continue to be deterred from disclosing sensitive information about disease outbreaks by political, economic, and personal costs. Such informational issues are not unique to global health.

a allison.carnegie@columbia.edu

b acarson@uchicago.edu

Other areas of international cooperation—from nuclear non-proliferation verification to the resolution of trade disputes—feature struggles to entice actors to disclose critical details.

One potential innovative solution involves secrecy. The creation of confidential information repositories in multilateral agencies can make individuals, firms, and governments more willing to share sensitive—and highly useful—information. When adopted, international institutions like the WHO can offer those "in the know" a safe and discreet way of sharing details in a limited way so that they do not reach a wide audience. Other issue areas with even more sensitivities underscore the role secrecy can play. The International Atomic Energy Agency, for example, has for decades offered confidentiality to states that divulge sensitive information about their own nuclear facilities or the nuclear programs of others. While states still may not share their most sensitive secrets, confidentiality measures in multilateral institutions can lower the barriers to information revelation, leading to timely information sharing about fast-moving problems.

This article applies insights about sensitive information and confidentiality to the context of global disease threats and describes findings that suggest that such measures may increase the effectiveness of cooperative efforts. We first review common reasons that states withhold important information about disease outbreaks and treatments. We then review lessons learned about similar informational dynamics outside of the public health context that suggest that confidentiality systems in international organizations (IOs) can address disclosure dilemmas. This analysis shows how sensitive information regarding international trade and intelligence about nuclear technology have been addressed by confidentiality. We then review new data on confidentiality measures that suggests that such procedures can improve IO effectiveness across a sample of institutions.

However, while confidentiality systems can elicit information, they are not panaceas. Better protection for information can only address problems that stem from the withholding of sensitive details about global disease outbreaks and treatment. Other problems that degraded the cooperative responses to COVID-19—including the distributional consequences from how information is used to inform policy actions—may well remain. We therefore conclude with some reflections on our study's relevance for the WHO and the importance of research and reforms that address the full scope of cooperation challenges for disease outbreaks.

TOO SCARED TO SHARE?

The under-provision and uneven distribution of information is widely recognized as an impediment to cooperation, as it permits states to avoid detection when they violate their agreements. In the broader study of international regimes and cooperation, compliant states fear that non-compliant states will exploit them, preventing them from cooperating in the first place.[1] In contrast, the reliable identification of failures to comply allows states to punish bad behavior, so that potential violators are frequently deterred.[2] Indeed, the literature on multilateral institutions has embraced this notion to such an extent that the critical role of "compliance information to facilitate compliance with international agreements" now constitutes "a centerpiece" of the study of international organizations in international relations (Dai 2002, 409).

As a result, empirical and theoretical analyses of global governance focus on conditions that produce transparency and accountability (Keohane 2006; Grigorescu 2007; Tallberg et al. 2014).[3] While scholars and policy-makers acknowledge a variety of information sources that can clarify compliance,[4] there has been less attention to the harm that disclosure can impose—and the resulting fear and reticence to share. In other work, we analyze fears of disclosure of commercially sensitive details and national intelligence that relate to questions of compliance about war crimes, trade, nuclear proliferation, and foreign investment (Carnegie and Carson 2020). In this paper, we address how allowing states to confidentially submit information related to disease outbreaks may improve the global response to these problems and other global issues.

There are multiple points during a disease outbreak when the failure to disclose sensitive information can endanger effective responses. During each, robust information sharing is necessary for timely action that can help contain outbreaks and save lives. Yet the financial, social, and security risks of these disclosures can delay them or prevent them from occurring at all.

At the beginning of an outbreak, the international community faces the challenges of identifying and tracking the disease. Doing so requires the prompt provision of health data. Knowledge of where a virus originates, how fast and through what pathways it spreads, and other information is critical to effective national and global responses. For example, sharing details about infected peoples' interactions and travel destinations is vital for tracing an outbreak's spread. With such information, the analysis of "big data" using sophisticated computational models can provide useful predictive power about a disease's movement and enable better containment efforts. Indeed, countries that have col-

1 See Keohane (1984); Mitchell (1998); Dai (2002); Voeten (2005); Lindley (2007).

2 Drawbacks to transparency may exist when states make diplomatic compromises (Stasavage 2004; Hafner-Burton, Steinert-Threlkeld, and Victor 2016), if it spurs others to defect (Lindley 2007), or for domestic reasons (Florini 2002).

3 Though see, e.g., Stone (2011).

4 See, for example, Dai (2002).

lected more information seem to have had more effective responses to their own outbreaks.

Yet such information is often sensitive and slow to see the light of day. Citizens may not report symptoms of the illness for fear of being quarantined, fired from their jobs, or socially stigmatized. They may also worry that their disclosures will allow data tracking during the pandemic or even be used for surveillance later. Scientists on the front lines can also serve as the eyes and ears for early detection, yet they too can suffer from providing information. For example, an Egyptian scientist working in Saudi Arabia was fired after sounding the alarm about the spread of the MERS coronavirus. As we discuss below, reforms at the World Health Organization have specifically attempted to create ways for scientific professionals to share information about disease outbreaks—underscoring the importance of nonstate actors in this context.

When national governments obtain information about an outbreak, their leaders may also decline to share it due to both economic and political concerns. Revealing an outbreak can lead to travel bans, visa restrictions, investment reductions, trade and capital regulations, and other negative ramifications. Data on particular regions or communities with high rates of infection can also result in discrimination.

Fears of information sharing also extend beyond the initial outbreak. Research into a disease's treatment and potential vaccines raises an additional set of sensitive information concerns. Here, information sharing and collaboration involves private pharmaceutical research by firms, academic research centers, and governments. Distribution of COVID-19 vaccines in the United States, for example, was slowed by poor information sharing between local, state, and federal levels about vaccine stockpiles, how to offer vaccine shots, and the rules for who should receive the vaccine.

In general, there often exist significant benefits to exchanging such information, as rapid scientific progress on treatment and vaccines can depend on collaboration among researchers. Countries benefit from sharing virus samples from all over the globe, for example. Disclosing genome sequences can also promote vaccine development and other efforts to combat viruses. Indeed, a Chinese laboratory that published the genome sequence of the coronavirus helped other scientists to develop new test kits.

Yet revealing research-related information comes at a significant cost. Private firms may sacrifice enormous potential profits—often needed to recoup the initial investment in their research—by revealing their data and discoveries. Their governments, moreover, may hope to capitalize on the market power and prestige that comes with developing a lifesaving treatment or vaccine. As a result, allegations of attempts to steal such information are common and show the stakes involved. Governments can also retaliate against individual scientists who try to share information. For example, the Chinese laboratory that published the genome sequence was shut down the next day.

Finally, once treatments and/or vaccines have been identified, sensitive information can be important for administering them. For example, if the WHO sends staff into the field to investigate or treat a disease, they may need information about a region's security situation to avoid conflict zones and ensure worker safety. Or they may require data on vulnerable populations where the disease can spread easily, such as those living in refugee camps. However, governments of countries in which the disease is spreading may balk at disclosing this information due to fears of domestic political damage or national security risks.

LOOKING TO DISEASE INTELLIGENCE

If governments or other actors will not disclose their own disease-related information, another option is for governments to share their knowledge of outbreaks in other countries. This idea has real potential: many countries invest in sophisticated intelligence-gathering capabilities, which can detect early signs of diseases through clandestine means.

Yet divulging such details can carry significant national security concerns for the government doing the disclosing. Sharing information based on sensitive intelligence sources and methods can allow surveillance targets to adapt their behavior to avoid detection. Other states may also learn more about the discloser's intelligence capabilities, which they can use to hide their illicit or controversial activities in other areas. Providing this information may also generate diplomatic blowback. Admitting to surveillance may be controversial, especially if it relates to a trade partner or geopolitical ally.

However, despite the high cost, supplying these details is necessary for a state's information to be considered credible. Relying on information from a third-party government raises the possibility that it has ulterior motives. Accusations may be seen as a form of political propaganda, or as a justification to impose punitive travel or trade restrictions. Intelligence regarding foreign outbreaks is therefore more credible when accompanied by clear sourcing and precise details.

The debate between the United States and China over how the COVID-19 outbreak started is instructive in this regard. Ambiguity about its origins remains despite this information's value in developing treatments and preventing future outbreaks. While China has been reticent to share information, the US claims to have intelligence that could shed light on this question.[5]

However, American claims are at least partly based on sensitive electronic intercepts of Chinese officials' internal discussions. Former president Trump publicly asserted that

5 We note that China likely has a variety of motivations for concealing disease Worsnop (2019), including domestic constraints and potential reputational consequences. Secrecy could help with some but not all of these concerns. For an overview of the literature on reputation, see Brutger and Kertzer (2018).

he was "not allowed" to reveal evidence linking the virus to a Chinese research laboratory, and public reporting suggests that providing such details "could well expose details of how the United States keeps track of Chinese leadership." As a result of the US's failure to enter such evidence into public discussion, others have dismissed these claims as mere propaganda.

Beyond intelligence, other forms of sensitive information could address other aspects of disease outbreaks. Consider, for example, data on vaccine development, access, and distribution. Local and national governments may fear publicly revealing information on vaccines for fear of endangering citizen privacy, exposing commercially sensitive information by pharmaceutical companies, or tipping their hand about a slow pace or excess supply. Yet obtaining such details may be vital to achieve a regional and global understanding of vaccine safety and effectiveness as well as its distribution to populations. Without a confidential way of disclosing such information, private-sector actors and governments alike may limit or entirely withhold details about disease response.

LESSONS FROM OTHER AREAS

Despite the extensive barriers to eliciting information about global health emergencies, the international community's experience in addressing other international challenges highlights how reforms to multilateral institutions can enable such sharing. Indeed, our research on sensitive information and cooperation challenges has identified similar forms of hesitation to share in domains like international trade, accountability for war crimes, and nuclear technology. In each, we found a surprisingly effective solution: empowering international organizations to receive, act on, and protect sensitive disclosures.

Consider how such systems can be used to help monitor compliance with international rules in domains like international trade and investment. In the trade arena, countries agree to rules that govern trade flows, but often disagree about whether specific government policies constitute violations of those rules. The World Trade Organization (WTO)'s dispute settlement process can help to adjudicate such cases, but may require affected parties to provide internal documents regarding their contracts, pricing, and costs. Doing so can be critical to establishing that a given policy put foreign firms at a meaningful disadvantage.

Not surprisingly, firms are often reluctant to divulge those details, fearing that they will be useful to competitors and endanger their market share. In response, the WTO developed ways to handle particularly sensitive information. For example, during a dispute about subsidies for the aircraft manufacturers Boeing and Airbus, the WTO implemented special procedures—stand-alone computers, a carefully controlled list of approved readers, and heavily redacted public reports—to ensure that sensitive internal data was kept in-house.

These kinds of systems can be effective for protecting disclosures not just from firms, but also from private citizens. Such a scenario is especially germane to disease outbreaks and response, where the infection and vaccination of individuals is a central issue of concern. This issue was addressed in the design of legal tribunals for war crimes. A recurring problem for those seeking to hold war criminals accountable is the need for, and sensitivity of, witness testimony. Documenting the "who," "what," and "where" of a wartime atrocity may require witnesses to share their experiences. Agreeing to testify, however, can put a witness's life in danger. International war crimes tribunals, like the International Criminal Tribunal for the former Yugoslavia, have thus developed ways to safeguard the anonymity of witnesses willing to testify.

Similarly, confidentiality systems have helped IOs that monitor weapons of mass destruction, such as nuclear technology (Carnegie and Carson 2019). Slowing nuclear proliferation often requires precise knowledge about which countries are developing nuclear weapons and details about their progress. Such information can be difficult to obtain; after all, countries often try to hide their illicit activities. Information from other countries' intelligence agencies can therefore prove critical to detecting these activities. Yet wide disclosure would tip off third-party state and nonstate actors about how intelligence is collected. This is particularly relevant to the disease context. Insights from intelligence agencies can be among the earliest pathways for outside actors to detect a disease outbreak, especially one in a low-information environment. In the American context, for example, a May 2020 report from the Congressional Research Service outlined a range of ways national intelligence assets are used for "disease surveillance."[6] Sources and methods concerns—whether intelligence is about disease or a nuclear enrichment plant—are relevant if such details are widely publicized.

In response to these challenges in the nuclear context, the International Atomic Energy Agency (IAEA) developed systems to ensure the confidentiality of such information, putting member states' disclosures about their own nuclear activities and those of others under lock and key. Doing so allows the organization to obtain more robust and honest information, which it uses to reach credible, publicly shared conclusions about nuclear activities. All the while, the IAEA keeps details about facilities and shared intelligence confidential, limiting the security or economic blowback that would result if this information were widely known.

These confidentiality protections have played an important role in some of the biggest nonproliferation successes. In 1991, the Persian Gulf War revealed that Iraq had hidden nuclear sites that were useful for nuclear weapons development. The IAEA encouraged other countries to securely share information, including that from sensitive intelli-

6 "Intelligence Community Support to Pandemic Preparedness and Response." CRS, May 6, 2020. https://sgp.fas.org/crs/intel/IF11537.pdf.

gence sources, to help it identify such sites. It did so using novel protocols for protecting such information from wide circulation. The IAEA's experts then relied on these disclosures and other information to investigate and document nuclear activities, giving the international community confidence that suspect nuclear sites were under control. This example highlights how sources and methods concerns—whether regarding intelligence related to disease or a nuclear enrichment plant—arise when insights gleaned from sensitive methods are widely known.

MULTILATERAL EFFECTIVENESS BY THE NUMBERS

These examples illustrate how equipping multilateral organizations with a secrecy capability can resolve disclosure dilemmas. But does this link between confidentiality and better institutional performance hold in a broader swath of issue areas and institutions? To assess the link between confidentiality and IO effectiveness, we assembled a dataset of fifty-three IOs and their information-related features. We followed the procedure used in Davis and Pratt (2017) to identify major IOs, since we expect our theory to apply best to these. We do not anticipate that our theory applies to smaller, club-style IOs, for example, because they may exist more for social purposes than for information dissemination. We thus expect our theory to generalize insofar as a given IO has a data collection and dissemination function.

Our dependent variable for this analysis is *IO performance*, taken from Lall (2017). This measure uses sets of indicators of whether IOs attain their goals, are cost-effective, and are responsive to diverse stakeholders. The indicators are drawn from official government assessments and are combined into a composite index using principal component analysis. Following Lall (2017), this variable is rescaled between 0 and 1.

To measure our key independent variable, we collected new data on whether international organizations possess confidentiality features. Other studies have gathered data on the transparency of IOs for non-state observers and the public communication activities of IOs.[7] However, given that our interest is in the presence of procedures for confidentially handling sensitive disclosures, we coded each IO according to whether it is equipped to protect shared data and documents.

We examined each IO's website, charter, disclosure policy, information sharing policy, secondary sources, and any other documents that discuss how the IO treated information that was provided by member states as of 2017.[8] In many cases this information was summarized in an IO's "Information Disclosure Policy" or "Information Sharing Policy." Broadly, these or their constituent documents discussed secretariat staff policies, organizational rules for access, and infrastructure for protecting sensitive details. They also often mentioned sensitive document storage methods, information transmission rules, and encryption and other IT protocols that were designed to protect sensitive information. Where available, we also consulted materials that described how documents were classified or labeled according to their sensitivity, which often included labels like "For Official Use Only," "Board-Approved Only," or "Business Confidential."

Using these materials, we coded whether each of the IOs in our dataset had any of the following: a document classification system that allows for classification by different levels of documents' sensitivity, staff policies for handling sensitive information including penalties for unauthorized disclosures, and designated physical or cyber storage facilities for sensitive information. An example of an economic IO with confidentiality protections is the Bank of International Settlements (BIS), as a set of 2014 BIS regulations allows submitted data to designate reported information as "Confidential statistical information, not for publication."[9] An example of a security-focused IO is the Organization for Security and Cooperation in Europe (OSCE). The Code of Conduct for staff from 2003 addresses sensitive sites and related information, stating that staff and mission members "shall at no time use, disseminate or publish information known to them by reason of their official position nor may they publish anything based thereon."[10] Since more kinds of secrecy do not necessarily increase effectiveness in a linear fashion, we dichotomize this variable to indicate whether any secrecy systems are present.

Following Lall (2017), our assessment of the impact on institutional effectiveness includes several covariates that address other factors that plausibly influence our dependent variable. First, we add *De facto policy autonomy*, which is an index that adds six indicators of IO agenda-setting abilities, decision-making procedures, and access to funding. These are each drawn from responses to an online survey in Lall (2017). We also include *Number of staff*, the logged number of full-time staff, to address variation in the size of IOs in our sample. We also add *Field presence*, which is a binary variable which takes a value of 1 if an IO has offices outside of the country in which it is headquartered, to address variation in the sprawl or compactness of institutions. Finally, we include *IO age*, the logged years post establishment, to incorporate the fact that institutions vary

7 On transparency in IOs, see Grigorescu (2015); Ecker-Ehrhardt (2018); Sommerer and Tallberg (2016).

8 We also consulted the charters for each IO, but they rarely featured explicit details about whether and how the IO protected sensitive information.

9 "Technical guidelines for reporting international banking statistics to the BIS." Version 3.0. February 2014. https://www.bis.org/statistics/bankstatsguide_tech.pdf.

10 "OSCE Code of Conduct for Staff/Mission Members," Appendix 1. June 2003. https://www.osce.org/secretariat/31781?download=true.

Table 1. IO Confidentiality & Performance, De Facto Autonomy

	DV: IO Performance
Confidentiality system	0.177***
	(0.061)
De facto policy autonomy	0.103***
	(0.033)
Number of staff (*log*)	-0.004
	(0.019)
Field presence	0.012
	(0.112)
IO age (*log*)	-0.045
	(0.042)
Constant	0.238*
	(0.134)
Observations	53
R^2	0.339
Adjusted R^2	0.268
Residual Std. Error	0.199 (df = 47)
F Statistic	4.815*** (df = 5; 47)

Note: *p<0.1; **p<0.05; ***p<0.01

considerably in their experience over time. Our specification replicates the results in Lall (2017) but adds our variable of interest—the presence of confidentiality provisions in an IO. Our analysis uses ordinary least squares with robust standard errors.

The results appear in Table 1. We find that, consistent with our expectations, the inclusion of confidentiality systems in multilateral organizations has a positive and significant association with IO performance. This is in line with our theoretical prediction that such systems improve IO functioning since they allow states, firms, and other actors to provide more sensitive information to the IO. This association is present even as we control for differences in the size, geographic reach, and age of institutions. Moreover, Lall's findings replicate: we find a positive and statistically significant association between IO autonomy and performance, suggesting that IOs with less interference from member-states are more effective in addressing policy problems.[11] These results are suggestive given data limitations, yet they corroborate our prior discussion.[12] While secrecy can be an awkward fit in global governance, these findings suggest that employing secrecy may improve multilateralism's effectiveness.

WHO TO THE RESCUE?

Having found a broad correlation between IO effectiveness and confidentiality, we return to the specific case of the WHO to discuss how these findings might be applied to pandemics. To date, the embrace of confidentiality in the global governance of public health has been partial at best. Some sensitive information regarding disease outbreaks is shared among governments with long-standing intelligence-sharing relationships. Further, many academic and private-sector researchers have built new collaborative relationships in seeking to respond to COVID-19. However, these measures cannot ensure an effective global response, and create information silos that duplicate efforts and expertise.

A necessary corrective is an international institution that can serve as a global repository for information and a leader in coordinating efforts to fight disease. A natural choice would be the World Health Organization, which constitutes a point organization in international health promotion and has emerged as a leader in pandemic situations. Taking on such a role, however, would require the WHO to follow the examples of the IAEA and other institutions by developing a reputation for securely storing sensitive disclosures and applying neutral, scientific judgments to them.

In some ways, the WHO is well-suited to institute such reforms. Indeed, the institution is staffed by experts and has had success using this expertise to eradicate diseases like smallpox and SARS. Moreover, while the WHO has few formal confidentiality provisions, the 2005 reforms codified in its International Health Regulations did include small confidentiality measures. For example, one article specifically provides the WHO with the authority to receive reports of disease outbreaks from non-state actors and allows the WHO to "maintain the confidentiality of the source." As a result, non-state actors frequently participate in identifying outbreaks and reporting them to the institution.

The WHO also has a culture of secrecy, refusing to release a variety of documents to the public and keeping states' information password-protected in order to maintain cordial relations with its members. It also relies on secrecy when deciding whether to designate an outbreak as a "public health emergency of international concern." The WHO Emergency Committee of experts, which assesses the merits of such a declaration, is "obliged to keep proceedings of meetings confidential, and not to disclose any documents or other information received." Such provisions help to encourage frank discussion and protect sensitive information.

11 See appendix for replication and extension using *De jure policy autonomy*.

12 See additional replication and extension finding in the appendix. Note that we cannot include IO fixed effects because our data provide a snapshot in time.

REFORMS TO REDUCE FEARS OF EXPOSURE

Despite the WHO's potential as a global leader in addressing the pandemic, convincing governments and private actors to share their sensitive information will not be easy. The knowledge gaps surrounding COVID-19 demonstrate that, long after the WHO's 2005 reforms, state and non-state sources of information still see significant risks associated with its disclosure. States frequently do not report outbreaks that occur in their own countries or in other countries, and often do not provide even basic information about diseases. Many details regarding treatments and vaccines also remain guarded.

Most importantly, trust that the WHO can protect confidential information must be improved before states, drug companies, and individual scientists will take risks in sharing it. This will be difficult, as the WHO was the subject of a widely reported cyber-attack in the early weeks of the COVID-19 crisis, and other leaks have occurred since then. The United Nations, of which the WHO is a part, is also notorious for leaks.

To improve trust, the WHO first needs to clarify and bolster its capacity to keep secrets. Outdated information technology infrastructures with simple password protections are not enough. The WHO could overhaul its technical capacities, with new hardware and improved software that can reliably encrypt sensitive details. This could be done in consultation with members, to ensure that the WHO's new systems meet members' expectations and allow them to feel comfortable sharing information.

The WHO should also redouble its efforts to develop a transparent and sensible system for classification levels, taking cues from national governments and other international institutions. Doing so can allow more tailored and reliable limits on who can view sensitive health-related information within the organization. Because information security ultimately relies on people, the WHO would also benefit from stiffening penalties for staff that do not properly safeguard this information.

A related challenge will be addressing broader accusations of bias and favoritism to build trust among states that doubt the WHO's independence and neutrality. The WHO praised China's handling of the COVID-19 outbreak even as China withheld information, leading to criticisms. Others frequently accuse the US of exercising undue influence over the institution, particularly given its outsized role in funding the WHO's activities.

Possibilities to improve trust include revised hiring and staffing practices to ensure that staff members come from relatively neutral countries. A more radical possibility is to spin off some functions of the WHO into autonomous activities or even a stand-alone entity. For example, the emergency response portion of the organization could take the lead on pandemic response, and could promote itself as being independent of the rest of the WHO.

In addition to efforts to encourage disclosures from member states, the WHO should continue to bolster its collection of information from non-governmental and open sources. Since 1998, the WHO has used its own contacts, diplomacy, and other open source information to collect data and has scaled up this collection during the recent pandemic. Such sources helped it to detect SARS in China despite a lack of information from Chinese representatives. While this kind of information cannot substitute for details and data from national governments, redoubled efforts to invite—and safeguard—submissions by non-official sources can still be critical to its mission.

THE DOWNSIDES OF SECRECY

While secrecy provisions can prove essential for eliciting information that fuels successful international cooperation, asking international bodies to keep secrets is not without risks. Concerns can arise about leaks, corruption, or general mishandling of such information. Indeed, there are significant benefits to transparency, as discussed in this issue in Adler and Kentikelenis (2022). The trade-offs we identify here mirror the trade-offs in transparent versus secretive diplomacy, an issue that has been debated for centuries.[13] Yet it is important to note that secrecy and transparency can often coexist, which can mitigate the risks to IO legitimacy that can accompany secrecy, as we discuss further below. Moreover, a variety of measures can be taken to significantly mitigate secrecy's potential downsides.

Consider the possibility of leaks. A provider of sensitive details may not feel comfortable sharing information if they fear that it will be compromised and end up in the public domain. This is not an unfounded concern; organizations have leaked confidential disclosures in the past. One particularly prominent example occurred in Somalia. Sensitive details that were shared with a peacekeeping mission in Mogadishu in the 1990s were exposed, prompting an outcry from the US Congress.

However, leaks often occur due to an institution's informal or flawed confidentiality systems. Secrets should not be shared with IOs unless and until they implement strict hardware and software protocols, through consultation and discussion with member states. The stronger these provisions, the more state and non-state suppliers will trust the IO to protect their sensitive information. If data is shared before such provisions are put in place, leaks can be difficult to avoid. The answer to concerns about leaks, then, may be more extensive secrecy capabilities rather than less.

Another risk in turning to secrecy is that states or other actors may worry that institutions will make corrupt or biased decisions. If institutions are not transparent and monitored, the argument goes, confidential disclosures could be used to advance individual or state-specific goals. Acting on information that cannot be shared widely may raise credi-

13 Mattingly (1988); Bjola and Murray (2016). For a review, see Carnegie (2021).

bility problems. Transparency therefore is often sought to permit accountability and prevent scandals.

One lesson from other institutions is that information disclosed confidentially can be backed up by non-sensitive details as an institution learns more. The IAEA has used sensitive information at the beginning of their inquiries into potential unreported nuclear activity; but, over time, it identified alternative forms of evidence derived from non-sensitive sources that could be shared with governments or the public.

Moreover, many forms of secrecy can coexist with transparency. Even if specific data or documents are kept under lock and key, the process governing what is kept secret, how confidential information is handled, and how it affects IOs' activities can remain transparent. The IAEA's reliance on shared intelligence, for example, led to critiques about possible bias. In response, the secretariat's staff redoubled efforts to make their process for using confidential details transparent to member states. Another measure to consider is tailored secrecy. Most documents can be revealed with redactions for specific confidential details. Indeed, IOs such as the WTO have made routine use of redactions for internal firm documents in their public reports.

Taking a page from democratic governments, international institutions can also reduce abuses of secrecy by adapting freedom of information-type rules. Such rules provide access to sensitive details months or years after their initial disclosure. Most disclosures lose their sensitivity with time as their relevance to current policies and political episodes dwindles and concerns about exposing cutting edge technology ease. Freedom of information systems help to deter the mishandling of sensitive details because secretariats and staff know that suspect activity will eventually come to light.

Moreover, secrets are only as good as the people who keep them. Ensuring that IO staff are vetted and approved by member states can help to engender trust. Institutions function best if they are staffed primarily by technocrats who have professional stakes in expertly handling sensitive information, rather than political appointees. In a multinational setting, it is also important to hire staff from a wide range of countries and experiences to avoid suspicions of bias or favoritism. The WHO has worked hard to build a reputation for apolitical judgments about disease. This trust in technocratic expertise may not suffer when adding confidentiality measures, as the World Trade Organization has shown for over a decade.

Finally, we note that secrecy is not a cure-all. While it can help states and other actors overcome hesitation to share information due to concerns about revealing sources and methods, it does not cause states to provide information when that provision is not in their interest. For example, if the conclusions that result from the information provision will harm the state, the state will never provide the information. Or, some leaders may have ideological opposition to international cooperation in the first place, like many populist actors. Nonetheless, secrecy can help in the important class of information withholding that we have identified.

CONCLUSION

Innovative solutions that elicit information from individuals, firms, and national governments are urgently needed. Yet the prospects for improving international responses to global health emergencies remain unclear. On the one hand, the urgency for action is high and continues to rise as health emergencies become increasingly global and complex. Epidemiologists warn that another global pandemic like COVID-19 is simply a matter of time. Climate change only deepens the certainty that other global health crises will stress institutions, economies, and societies.

Yet crisis can open up opportunity. For example, difficult reforms to protect sensitive disclosures at the IAEA came only after the dramatic exposure of hidden nuclear developments in Iraq in 1991. The COVID-19 crisis may be the spark that lights enough political will to implement dramatic changes at the WHO or to create a parallel institution. Additionally, non-governmental organizations such as the Bill and Melinda Gates Foundation could step in. These groups have often helped to finance global health initiatives when governments fall short, and many are adjusting their funding priorities to address current and future pandemics.

On the other hand, there are limits to what confidentiality can do and whether such reforms may be possible. Disclosure dilemmas are not the only barrier to cooperation that affected responses to COVID-19 and other disease outbreaks. Governments and pharmaceutical companies may also be concerned about how information is used rather than the method of sharing. Multilateral assessments and decisions about the origins of an outbreak, its danger to other countries, and the methods of treatment create winners and losers. Such distributional concerns will continue to pose problems, even if confidentiality reduces one important barrier to information sharing.

Another factor is the broader political climate. The responses to COVID-19 makes it clear that some political leaders and groups see political opportunity in criticizing the science of disease outbreaks as well as responses like masking and vaccination. Such populist, anti-science sentiment will make reforms that address confidentiality less likely. Moreover, other aspects of political will may not favor reforms that facilitate sensitive information sharing. Even if NGOs chip in, government funding will still be needed, and may be in short supply given the WHO's reliance on voluntary contributions. After all, the economic cost of the pandemic has led governments to tighten, not expand, their budgets. The optics surrounding reform constitute an additional reason for pessimism. Calls for transparency are often more politically palatable than redoubling efforts to protect sensitive information with secrecy.

Finally, the turbulence of American leadership at institutions like the WHO under the Trump and then the Biden administration complicates potential reform efforts. Instead of change, paralysis may be the by-product of the US-China dispute about COVID-19, the criticism of early WHO decisions, and disagreements about vaccination equity. While it is possible that President Biden and future presidents will

revitalize US leadership at the WHO and other multilateral venues and ease disputes with China, this remains to be seen.

Even if these challenges can be overcome, leaders must recognize and embrace the urgency of eliciting sensitive information through measures like secrecy. We live in an information age in which digital and communication revolutions have led to seemingly endless access to knowledge. A tragic—and ironic—lesson of the COVID-19 pandemic is that such information is grossly insufficient. If governments, firms, and citizens remain afraid to provide the vital details needed for identifying, slowing, and treating outbreaks, then the next pandemic will unfold with similarly devastating consequences.

AUTHOR BIOS

Allison Carnegie is Associate Professor (with tenure) of Political Science at Columbia University. She serves as the Director of Graduate Studies and Director of the Politics and the Global Economy (PaGE) Lab. 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. She is the author of *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation* (Cambridge University Press, 2020) with Austin Carson and *Power Plays: How International Institutions Reshape Coercive Diplomacy* (Cambridge University Press, 2015). Her work has been published in a variety of outlets including the *American Political Science Review, American Journal of Political Science, British Journal of Political Science, International Organization, Journal of Politics*, and *Political Analysis*.

Austin Carson is Associate Professor of Political Science at the University of Chicago. He is the author of *Secret Wars: Covert Conflict in International Politics* (Princeton University Press, 2018) and *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation* (Cambridge University Press, 2020, coauthored with Allison Carnegie). 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.

COI STATEMENT

The authors have no competing interests to declare.

ACKNOWLEDGMENTS

Donald Casler, Richard Clark, and Maya Van Nuys provided excellent research assistance. All remaining errors are our own.

Submitted: January 31, 2022 PST, Accepted: September 21, 2022 PST

REFERENCES

Adler, David R. K., and Alexander E. Kentikelenis. 2022. "Pump Up the Volume: From Covert to Overt Politics in Global Governance." *Global Perspectives* 3 (1): 55675. https://doi.org/10.1525/gp.2022.55675.

Bjola, Corneliu, and Stuart Murray. 2016. *Secret Diplomacy: Concepts, Contexts and Cases*. Routledge.

Brutger, Ryan, and Joshua D. Kertzer. 2018. "A Dispositional Theory of Reputation Costs." *International Organization* 72 (3): 693–724. https://doi.org/10.1017/s0020818318000188.

Carnegie, Allison. 2021. "Secrecy in International Relations and Foreign Policy." *Annual Review of Political Science* 24 (1): 213–33. https://doi.org/10.1146/annurev-polisci-041719-102430.

Carnegie, Allison, and Austin Carson. 2019. "The Disclosure Dilemma: Nuclear Intelligence and International Organizations." *American Journal of Political Science* 63 (2): 269–85. https://doi.org/10.1111/ajps.12426.

———. 2020. *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation*. Cambridge University Press. https://doi.org/10.1017/9781108778114.

Dai, Xinyuan. 2002. "Information Systems in Treaty Regimes." *World Politics* 54 (4): 405–36. https://doi.org/10.1353/wp.2002.0013.

Davis, Christina L., and Tyler Pratt. 2017. "The Forces of Attraction: How Security Interests Shape Membership in Economic Institutions."

Ecker-Ehrhardt, Matthias. 2018. "International Organizations 'Going Public'? An Event History Analysis of Public Communication Reforms 1950–2015." *International Studies Quarterly* 62 (4): 723–36. https://doi.org/10.1093/isq/sqy025.

Florini, Ann M. 2002. "The End of Secrecy." In *Power and Conflict in the Age of Transparency*, edited by Bernard I. Finel and Kristin M.Lord Palgrave.

Grigorescu, Alexandru. 2007. "Transparency of Intergovernmental Organizations: The Roles of Member States, International Bureaucracies and Nongovernmental Organizations." *International Studies Quarterly* 51 (3): 625–48. https://doi.org/10.1111/j.1468-2478.2007.00467.x.

———. 2015. *Democratic Intergovernmental Organizations? Normative Pressures and Decision-Making Rules*. Cambridge University Press.

Hafner-Burton, Emilie M., Zachary C. Steinert-Threlkeld, and David G. Victor. 2016. "Predictability Versus Flexibility: Secrecy in International Investment Arbitration." *World Politics* 68 (3): 413–53. https://doi.org/10.1017/s004388711600006x.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press.

———. 2006. "Accountability in World Politics1." *Scandinavian Political Studies* 29 (2): 75–87. https://doi.org/10.1111/j.1467-9477.2006.00143.x.

Lall, Ranjit. 2017. "Beyond Institutional Design: Explaining the Performance of International Organizations." *International Organization* 71 (2): 245–80. https://doi.org/10.1017/s0020818317000066.

Lindley, Dan. 2007. *Promoting Peace with Information: Transparency as a Tool of Security Regimes*. Princeton University Press. https://doi.org/10.1515/9780691224251.

Mattingly, Garrett. 1988. *Renaissance Diplomacy*. Courier Corporation.

Mitchell, Ronald B. 1998. "Sources of Transparency: Information Systems in International Regimes." *International Studies Quarterly* 42 (1): 109–30. https://doi.org/10.1111/0020-8833.00071.

Sommerer, Thomas, and Jonas Tallberg. 2016. "Transnational Access to International Organizations 1950–2010: A New Data Set." *International Studies Perspectives* 18 (3): 247–66. https://doi.org/10.1093/isp/ekv022.

Stasavage, David. 2004. "Open-Door or Closed-Door? Transparency in Domestic and International Bargaining." *International Organization* 58 (04): 667–703. https://doi.org/10.1017/s0020818304040214.

Stone, Randall W. 2011. *Controlling Institutions: International Organizations and the Global Economy*. Cambridge University Press. https://doi.org/10.1017/cbo9780511793943.

Tallberg, Jonas, Thomas Sommerer, Theresa Squatrito, and Christer Jönsson. 2014. "Explaining the Transnational Design of International Organizations." *International Organization* 68 (4): 741–74. https://doi.org/10.1017/s0020818314000149.

Voeten, Erik. 2005. "The Political Origins of the UN Security Council's Ability to Legitimize the Use of Force." *International Organization* 59 (03): 527–57. https://doi.org/10.1017/s0020818305050198.

Worsnop, Catherine Z. 2019. "Concealing Disease: Trade and Travel Barriers and the Timeliness of Outbreak Reporting." *International Studies Perspectives* 20 (4): 344–72. https://doi.org/10.1093/isp/ekz005.

APPENDIX

Table 2. Replication of Model 6 (Lall 2017): De Jure Policy Autonomy and IO Performance

	DV: IO Performance
De jure policy autonomy	0.018
	(0.024)
Number of staff (*log*)	0.005
	(0.018)
Field presence	-0.065
	(0.118)
IO age (*log*)	-0.014
	(0.051)
Constant	0.522***
	(0.139)
Observations	53
R^2	0.029

Note: *p<0.1; **p<0.05; ***p<0.01

Table 3. IO Confidentiality & Performance: Extension of Lall 2017 (De Jure Autonomy)

	DV: IO Performance
Confidentiality system	0.192***
	(0.069)
De jure policy autonomy	0.011
	(0.023)
Number of staff (*log*)	-0.007
	(0.019)
Field presence	0.005
	(0.108)
IO age (*log*)	-0.027
	(0.048)
Constant	0.480***
	(0.144)
Observations	53
R^2	0.165

Note: *p<0.1; **p<0.05; ***p<0.01

Table 4. Replication of Model 6 (Lall 2017): De Facto Policy Autonomy and IO Performance

	DV: IO Performance
De facto policy autonomy	0.111***
	(0.035)
Number of staff (*log*)	0.007
	(0.019)
Field presence	-0.053
	(0.125)
IO Age (*log*)	-0.035
	(0.048)
Constant	0.274**
	(0.136)
Observations	53
R^2	0.224

Note: *p<0.1; **p<0.05; ***p<0.01