Secrets and Secrecy

The Case for a Practitioner's Dialogue

Joseph Gartin and Timothy Schulz

Joseph Gartin is a retired CIA officer and past managing editor of *Studies*. Timothy Schulz is a program manager in the Center for the Study of Intelligence.

"Tell me the secret that you possess."

"I will not, for this is in my power."

Epictetus, *Discourses*

Writing about government secrets and secrecy is irresistible, judging from the many books, scholarly articles, industry publications, and commentaries that now treat the US Intelligence Community. With varying degrees of accuracy and thoughtfulness, many of these works make broadly similar arguments: The US government over-classifies information (Hathaway, Lebovic, Maret); It relies too much on secrecy and secrets in the conduct of national security decisionmaking and actions (Brown, Connelly, Monyihan); and publicly available information increasingly supplants secrets (Zegart). More advice comes from prominent think tanks, which argue the IC needs to step out from behind the wall of official secrecy and embrace new, more open ways of doing business (Weinbaum, et al.). A small but important body of academic work in recent years has tackled the thorny ethical considerations around state secrecy (Fabre, Ben Jafel, Pozen), building in part on foundational scholarship (Sissel, Shils, Bok), and wrestled with epistemological questions applied to intelligence analysis (Whitesmith).

This list is hardly exhaustive, as the explosive growth in intelligence literature in the past two decades shows (Coulthart, Rorissa), but it represents the broad contours of mainstream, English-language discourse about secrets and secrecy in the IC. Although one can point to flaws in some of the arguments for and against secrecy in intelligence, taken together they highlight an opportunity for practitioners.

In this essay, we argue secrets and secrecy are naturally integral to intelligence, and yet neither is subject to rigorous evaluation by those who create and value them most. We explore the reasons behind this gap, examine the carrying and epistemic costs of secrecy, contest arguments against government secrecy, explore potential analogs that could help inform the IC's relationship to secrets and secrecy, and suggest areas of further research.

Before proceeding, it is useful to define some terms. Secrets are bits of information that are willfully withheld. As we will discuss in detail, secrets are not fixed things; they shift in response to changes in perceived value of openness versus privacy. The reader does not know what we had for breakfast. That is not a secret, because there is no perceived value in concealing or revealing the information. On the other hand, if readers wanted to poison our breakfast because they are our mortal enemies, they would conceal their intention and capability; if we knew either bit of information, we would conceal our dining habits.

Turning to secrecy, we observe at least three senses of the word and their relationships to one another. The first is the willed act of nondisclosure: to make, hold, or selectively share a secret is to engage in secrecy. We call this base definition act-secrecy. This is the everyday sense of the word. A person or group decides not to let someone know a piece of information.

Secrecy also points to a normative system prescribing, regulating, or often dominating a member's disclosive or non-disclosive calculus. This system-secrecy appears as an epistemic and social arrangement. The system must judge the default status of information: What newborn information can pass into discourse, what falls secret, and who decides?

But secrecy can also refer to something much larger than mere secret-keeping. Secrecy also points to a type of normative system. It is normative because it prescribes or regulates information disclosure and non-disclosure, circumscribes the individuals or types of people who can be admitted into the system and occupy roles within it, and describes the sanction regime for violations. Unlike act-secrecy, system-secrecy is an epistemic and social arrangement. One of its main epistemic tasks is determining the default status of newborn information. That is, what can pass into discourse, what falls secret, and what must be adjudicated one way or the other. The system must also decide the individuals or sorts of individuals who have the power to modify and regulate the system of secrets—this is a political and social decision as much as a counterintelligence or bureaucratic concern.

A third sense of secrecy is constitutive-secrecy, i.e., an organization's attempt to constitute itself in the larger political sphere. The "Glomar response"—neither confirm nor deny—is emblematic of this constitutive-secrecy.[a] Glomar is not in the first instance about information nor about a system aimed at handling secrets. It is an organization's attempt to define itself by its secrecy. If one were to ask the tax agency for another's tax records, the agency would simply say "no." If one were to ask an intelligence organization for secret records, the Glomar response conveys to the requester that the IC is not the sort of place that discloses its business. Glomar does not keep a secret so much as foreclose inquiry into the possibility of a secret.

a. The term is taken from revelations of Project AZORIAN, in which the Hughes *Glomar Explorer* was used in a covert, CIA-led attempt to recover a sunken Soviet submarine in 1974.

Dominating Characteristic

Secrets and secrecy are as necessary to protect political communities as they are to protect individual liberty. Unlike some outside the IC, we do not assert *a priori* that the IC abuses secrecy, and we reject as indefensible the premise that secrecy is unnecessary in today's global information environment or that secrecy is incompatible with liberal democracy. Essential functions of government, including but not limited to the national defense (for example, setting interest rates or negotiating contracts), would be impossible without the capacity to keep some secrets. That said, the weight of secrecy is heavy.

Reviewing Sissela Bok's *Secrets: On the Ethics of Concealment and Revelation* in these pages in 1984, John Harington observes that secrecy is "the dominating characteristic of intelligence work, whether it is a question of the safeguarding or compromise of one's own secrets or the acquisition by stealth of another."[a] Of course, governments are not alone in keeping or seeking secrets. Secrets and secrecy, Bok argued, are essential for individuals and the state alike. They preserve the physical, emotional, and temporal space necessary to make decisions and safeguard the privacy and intimacy needed for human coexistence.

Forty-plus years on, however, we would argue secrecy is not only the how of intelligence, as Harington observed, but the what. Like the old saw about one young fish asking another as they swim along—"What is water?"—today's intelligence practitioners are so immersed in secrets that they cannot readily distinguish between secrecy as an act, culture, process, or outcome. Prying these differences apart would enable a constructive dialogue owned by practitioners.

Secrets of the State

For centuries, *arcana imperii*—the mystery of rule—meant state secrecy was largely immune to checks and balances, and the arguments against openness redound across epochs, regions, or polities. Leaders of every stripe have assiduously held to the principle that secrecy is essential to the exercise of executive power, that total transparency is impossible given human nature, and that the sovereign alone can determine what is and is not secret. We need look no further than the Founders' defense of secrecy during the American Revolution. George Washington argued, "All that remains for me to add is, that you keep the whole matter as secret as possible. For upon Secrecy, success depends in most Enterprises of the kind, & for want of it, they are generally defeated, however well planned." (Quoted in Lathrop)

Despite the continuity of this logic across history and forms of government, some political communities have gradually if grudgingly imposed limits on state secrecy. Within the United States, for example, construction of these guardrails began in earnest in the 1970s, driven by a changing media environment, abuses of executive power, revelations of unlawful intelligence and police activities, and evolving norms for legislative oversight. Since then, successive cycles of revelation and response in the late 20th and early 21st centuries ushered in a complex array of laws, policies, and procedures that partially constrain intelligence agencies' inherent capacity to abuse secrecy.

We stress inherent, because what is remarkable about secrecy in the US Intelligence Community is the extent to which it is not abused, given its enormous capacity and capability. (To be sure, ours is a contested viewpoint.) We emphasize partially because this state of restraint is entropic; history shows that maintaining the status quo depends on norms and behaviors that can change, often suddenly, under external or internal influences.

Habits of Secrecy

The place to begin this examination is with secrecy itself. Individuals and groups of all kinds—families, social networks, private societies, cults, congregations, corporations, and governments—keep secrets. For

a. John Harington, review of Sissela Bok, *Secrets: On the Ethics of Concealment and Revelation* (Pantheon Books, 1982), *Studies in Intelligence* 28, No. 2 (Summer, 1984).

individuals, habits of secrecy are learned at a very young age, as centuries of fiction have explored: secret powers, friends, languages, forests, labyrinths, and portals, to name a few. Imagine *The Lion, the Witch, and the Wardrobe* without a secret doorway to Narnia, *Harry Potter* without his invisibility cloak to move secretly through the corridors of Hogwarts, or *Harriet the Spy* without her secret notebook filled with information about her classmates and neighbors. Scholars have further observed that, for children, secrets and the physical or mental spaces they create offer power in the face of omnipresent vulnerability. (Sturm, Bosman, and Lambert)

Indeed, power and vulnerability are at the very heart of act-, system-, and constitutive-secrecy. Bok observed, "Some capacity for keeping secrets and for choosing when to reveal them, and some access to the underlying experience of secrecy and depth, are indispensable for an enduring sense of identity, for the ability to plan and to act, and for essential belongings. With no control over secrecy and openness, human beings could not remain either sane or free." This is true, we would argue, whether the secrets belong to a child or a government.

Secrecy exists in every level and every role of government decisionmaking, but it naturally has an outsized role in national security enterprises, where power is concentrated in the executives. We need not look very hard to find examples from history:

- During the Warring States (403–221 BCE) period in China, strategist Lu Shang advises, "In employing the army, nothing is more important than obscurity and silence. In planning, nothing is more important than not being knowable. The greatest affairs are not discussed, while the employment of troops is not spoken about."[a]
- In his history of Rome's tumultuous Year of the Four Emperors (69 CE), Tacitus recounts how the short-lived emperor Marcus Otho Caesar Augustus rebuked his soldiers: "We are preparing for war. Do you imagine that we could publish all our dispatches, and discuss our plans in the presence of the whole army, when we have to devise a systematic campaign and keep up with the rapid changes of the situation? There are things a soldier ought to know, but there is much of which he must be ignorant."[b]
- Fifteen hundred years later, Giovanni Botero, the great sixteenth-century adviser to Italian courts, observes, "Secrecy is also of great importance to a prince; not only does it make him like God, but men, ignorant of his intentions, are kept in suspense about his schemes."[c]

Pathologies

If secrets and secrecy are endemic to governments and essential to freedom of action, they are also at the heart of every kind of institutional scandal: torture of prisoners, polluted drinking water in poor neighborhoods, medical experimentation on the unwitting, abuse of children, and so on. Unifying these disparate attacks on human dignity, which disproportionately affect the weakest among us, are the mutually reinforcing pathologies of unchecked secrecy in powerful institutions:

- Absolute executive authority over secrecy, whether by decree, assent, or tradition.
- Expansive scope and depth of what institutions might consider secret, including membership, rites, knowl-

a. Cited in Ralph D. Sawyer, "Traditional Chinese Conceptions and approaches to Secrecy, Denial, and Obfuscation," *Studies in Intelligence* 64, No. 1 (March 2020).
b. Tacitus, *Histories*, Loeb Classical Library (1925). www.penelope.uchicago.edu/Thayer/E/Roman/Text/Tacitus/Histories/2A*.html.
c. Giovanni Botero, *The Reason of State,* trans. Peter Joseph Waley and Daniel Philip Waley (Yale University, 1956), 56.

edge, ignorance, capabilities, and intentions.

- Absence or impotence of channels for appeal or arbitration.
- Weakness or complicity of counterbalancing institutions, like the police, civil society, press, or courts.
- Wide-ranging, often lifelong, strictures against revealing secrets.
- Coercive tools to enforce secrecy, including censorship, banishment, garnishment, imprisonment, torture, and death.

Hesitancy among practitioners to critically examine secrecy is driven by three broad factors. First, intelligence services worldwide generally see secrecy through the lenses of security, compliance, and authority. Bok observed that "keepers of secrets can experience the powerful, the forbidden, and the sacred with the same awareness that outsiders have of such secrets as both endangered by and dangerous for those who come too near or who expose them." This esoteric relationship with secrecy, she argued, "inheres in the sense of sacredness that people can have with respect to themselves, their families, their professions, their nations. It serves as an indispensable function in protecting these, but it can also deflect moral inquiry."[a]

Within secret organizations, the esoterica of system-secrecy manifests in multiple ways: extensive barriers to entry, such as testing, vetting, and training; ritualized introductions to secrecy through ceremonies, oaths, and documents; the adoption of new identities; messaging that equates employer to family; rigid, vertical lines of authority over what is and is not secret; arcane segmentation of the population into in and out groups; and isolation from the public common.

These combine, intentionally or not, to stifle vigorous debate, and this is acutely so within intelligence services. The immutable connection between intelligence (the what) and secrecy (the how) leaves the practitioner with little intellectual space to evaluate its impact or to offer alternatives. At best, such efforts look quixotic; at worst, they may be perceived as professionally fraught.

Secrecy Besieged?

Second, intelligence practitioners are naturally inclined to dismiss calls for less secrecy and more openness as risky, impracticable, or even malicious. As a result, IC insiders have largely ceded the intellectual conversation to non-practitioners in media and academia. This is not to devalue those perspectives, as our bibliography indicates, but rather to observe that intelligence officers often reflexively reject challenges to secrecy. Writing in 2011, for example, Bowman Miller calls WikiLeaks "an aberrant manifestation of transparency advocacy" that had turned "the whole notion of operational security and protection of sensitive sources" on its head. Miller doubles down, arguing that the ability to keep secrets is endangered.[b]

Miller's claim conflates act-secrecy (creating a secret) with system-secrecy (keeping a secret), and in either case it is contradicted by the explosion in intelligence collection 15 years on. However prevalent the view of secrecy as besieged, the simple fact is that worldwide, intelligence agencies are keeping vastly more secrets, not fewer, and nothing has slowed the growth.

The principal challenge today is not that states cannot keep secrets, rather that governments must collect, store, and safeguard exponentially greater numbers of secrets. The accumulation occurs as both an intentional outcome (e.g., disseminated analysis) and as a waste product, in the same way that mining a small amount of gold results in vastly disproportionate amounts of worthless, toxic tailings that must be retained for

a. Bok, *Secrets*, 39.
b. Bowman H. Miller, "The Death of Secrecy: Need to Know…With Whom to Share," *Studies in Intelligence* 55, No. 3 (September 2011).

generations. Every new seam of secret information adds to the pile.

Disparate Obligations

Finally, the third factor is the traditional separation (at least in the US system) between the provider and consumer. We mean more than the generally accepted divisions of labor for reasons of efficiency, expertise, and security, or the divide between policymaker and analyst to safeguard objectivity. Instead, we emphasize the gap in ethical duty. The IC is left to ensure that the acquisition of the secret meets the ethical tests—do we really need it or will it answer a question we have?—along with any legal requirements for lawful collection. In contrast, consumers of intelligence need only to concern themselves with reliability and utility.

Truth to Power

A further challenge in fostering a conversation about secrecy is IC messaging and lore, which tend to equate secrecy with truth. We need look no further than the inscription from John 8:32 inside the entrance to CIA's headquarters: "And ye shall know the truth, and the truth shall set you free." (The critical context is missing: Jesus was disclosing His divine nature.) Similarly, every IC officer knows the mantra that the community should "speak truth to power," echoing an eponymously titled Quaker pacifist treatise published in March 1955. And yet, the IC does not possess the truth. It works to build understanding and to deny the same to others. Secrecy enables and hinders those goals.

A deep dive into theories of truth is well beyond the scope of this essay. It is sufficient to observe that there is a difference between truth as a comprehensive understanding of the world and facts as the basic units of truth that the IC collects, assesses, and uses to promulgate contingent knowledge. Perfect collection would yield all the secrets, but we might still lack all the relevant facts and the understanding formed by their correct ordering. This is because secrets are not facts; they might not even be true, but rather falsehoods, half-truths, and outright deceptions (like Curveball's fabricated reporting on Iraqi weapons of mass destruction).

For intelligence practitioners, the truth-to-power expression embodies truths in the furtherance of a state's interests. Scholars have emphasized that objectivity in intelligence is inherently elusive because no intelligence officer approaches the task without significant cognitive biases. (Marrin) In the United States specifically, these biases reflect a general if sometimes uneasy elite consensus formed and refined in the mid-to-late 20th century and further adapted to the post-9/11 world. This consensus historically saw the United States as a superpower shaping the international order and defending liberal democratic institutions. There is nothing universal about this consensus; analysts in Beijing, Moscow, New Delhi, or Brasilia will approach the truth-to-power responsibility in vastly different ways.

This is not to subscribe to a kind of relativism, but rather to stress that even intelligence truths are relationships with propositions, and those relationships are more fluid than practitioners generally acknowledge. Take for example Usama bin Ladin's safe haven in Abbottabad, Pakistan, in spring 2011. Known but to him and the inner circle that protected him, the fact of his location was transformed into a secret by his need to keep it from us. In turn, for the United States, Bin Ladin's presence was not understood at the time as a fact, even though it was ultimately true. It was at best a proposition.

Contingency

Abbottabad reminds us that secrecy is a value model between discovery and concealment. This contingency depends on a relationship between parties who keep or seek secrets, often both at once. The long hunt for Bin Ladin was an interplay between prey and pursuer, with each side shifting between those roles, along the way creating, protecting, and discarding secrets. For those in the know, Abbottabad was an unmentionable secret, then in a blink, it was not.

What changed was the value of withholding versus revealing the information, not the fact itself. In essence, the secret of Abbottabad was demonetized by Bin Ladin's death.

For intelligence practitioners, however, the idea of contingency is naturally fraught. For one, keeping secrets is exceptionally difficult even within secret organizations. The temptation to share a secret can be overwhelming; once loosed it spreads exponentially. How many times has an intelligence officer said or heard, "this is close hold, but…"? Extending Sissel's argument, the need to know clashes with the brief thrill of sharing, whether gossiping online or in a sensitive compartmented information facility, in the way that we most treasure some precious object the moment we lose it.

Carrying Costs

One effect of this blurring is to obscure the substantial costs of secrecy imposes, beginning with carrying costs. There is some hazard in trying to apply business models to government activities, but intelligence is a commodity like any other. It requires capital and labor to produce, and this production involves carrying costs: property, maintenance, depreciation, training, insurance, warehousing, etc. States, institutions, or groups require hierarchy, rules, norms, infrastructure, and workers to gather, assess, sort, distribute, and store secrets. The more expansive security organizations become, the more banal their records. Witness the trivial but thorough documentation of citizens' daily lives by domestic spy agencies in East Germany or Albania, among others, whose mundane secrets spilled into the streets when their authoritarian governments collapsed. (Garton Ash, Ypi) Intelligence organizations need the capacity to gauge requirements for new secrets, prevent theft or chase down leakers and spies, deflect inquiry, vet those who may need access, or selectively divulge secrets. (Pozen)

We can think of this as system-secrecy, with its complex interplay of internal and external forces affecting an ever-shifting population of secrets. In the United States, this system began to take shape at scale during World War I with the passage of the Espionage Act of 1917, faltered in the interwar years, and established a permanent foothold after World War II with the National Security Act of 1947 and subsequent legislative and executive actions. Eight decades on, it is a colossus. As one former policymaker noted, in 2017—the last year for which data are official and public—roughly four million Americans with security clearances classified some 50 million documents at a cost of around $18 billion. (Hathaway)

Furthermore, we can reasonably postulate that these reflect only direct costs. A complete accounting is utterly impossible because secrets come in a variety of forms: tangible goods, like documents, records, and physical property, of course, but also intangibles like identities, memories, relationships, knowledge, plans, intentions, and desires. However one measures them, the costs of secrecy last multiple generations and inevitably grow over time. Just as we cannot calculate the costs of existing secrets and secrecy, there is no estimate of their future costs in the national security realm. In budgetary terms, we might think of them as a deferred obligation akin to social service programs or infrastructure repairs.

Health Care Analogy

To understand the enormity of future carrying costs, we looked for analogous problems. One is the cost of providing veterans' health care in the United States. Like secrets, wars create a bow wave of future expenses; unappropriated for in the present, they must be reckoned with eventually. For example, according to a prominent scholar, Veterans Administration expenditures for World War I veterans peaked in 1969, 50 years after the armistice, and those for World War II veterans crested in 1982. (Bilmes, 2011) Her updated estimates of total health-care costs for 9/11-generation veterans (2001–21) are upward of $2.5 trillion in 2050. These costs grow because the complexity of veterans' healthcare needs increases with age even as the number of

living veterans in the cohort gradually declines and eventually reaches zero. (Bilmes, 2021)

This analogy only takes us so far, however, because unlike generational cohorts that can be projected over time with a high degree of actuarial confidence, secrets are unbounded cohorts that move along multiple axes. Put more bluntly: all veterans eventually die; secrets live on. One might, for example, first array secrets along an x-axis of *time* and a y-axis of *value*. To this simple quadrant we might add a third dimension: *volume*. The complexity of our mental graphic grows if we consider that an individual secret's placement is not fixed. A secret's importance can grow or fade, for example, and new secrets alter old.

Moreover, we can attribute value to secrets in their final states and in their constituent elements. In other words, if a chocolate chip cookie is a secret, so too are the ingredients (flour, sugar, eggs, etc.). But it doesn't end there. Much like the coastline paradox, in which the fractal properties of a coastline make it hard to decide on the minimum feature to be measured, secrets spawn geometrically more secrets. Thus, our secret cookie also means secrets about recipe testing, marketing strategies, social media data, pricing, demand, production rates, customers, packaging, supply chain vulnerabilities, competitors, corporate ambitions, and so forth. Acknowledging that there are many uncertainties and variables that will affect the future cost of safeguarding today's secrets, it seems likely that transactional costs will grow as the volume of information grows.

Epistemic Costs

In addition to carrying costs, we think practitioners should also confront the non-monetary costs of secrecy. Knowledge is central to intelligence, and so first among secrecy's non-monetary costs is its effect on the formation and distribution of knowledge. The fuzzy consensus among epistemologists carves up knowledge into justified true belief, absent spoilers. Setting aside justification and spoiler cases as worthy of their own investigation in other forums, we focus simply on true belief.

Secrecy in the first instance aims to prevent some particular person or group from forming a belief. The trouble is that secrets cannot themselves discriminate. Secrecy keeps the intended *incognoscenti* in their darkness along with all else who lack formal and actual access. Formal access bypasses act-secrecy; a person has the clearance to be informed and thereby update his beliefs. But system-secrecy also requires informal access. Contrary to popular depictions or questions from family back home, there is no secret scrolling ticker on our screens or Big Book of Cool Secrets we receive after the oath of office. Secrets in a system move strangely or not at all compared to the chatter of ordinary life. Practitioners must recognize a gap in their beliefs or the beliefs of others and know what office, system, or person might fill it. In a sprawling enterprise like the IC, this is not trivial.

A would-be knower's belief must be true. For some questions, achieving a true belief is straightforward, even if difficult. "Is Bin Laden in Abbottabad now?" enjoys strict bivalence: it is either true or false. This type of thin question—one person, one place, one time—can be consequential for the IC, but more often, intelligence questions are conceptually thick. "Is the regime stable?" brims with possibilities. The question decomposes into a host of individual propositions: a line of boxes that must be filled with true beliefs individually to reach a true belief about the regime's stability collectively. These boxes are roughly joined by conjunction, meaning that a top-line true belief is achieved by the truth of the series of propositions {A and B and C and D and… N}. A single false belief could be a spoiler for epistemic success.

Secrecy acts like a tax on each individual proposition in a conceptually thick intelligence question. The obvious tax is the secrecy of our adversary. This tax is often transparent, however. We often know we have seen through the secrecy or we have not. Within the IC, secrecy (and functional

specialization) distributes information unevenly across departments and agencies, but is it difficult to account for exactly how. The secrecy of compartmentalization, multiple computer networks, and the core sources-and-methods protections interfere with true belief formation by blocking-access to information as a default position.

Susan Maret gives us a more elegant vocabulary for the problem of information distribution within the IC. Writing in the journal *Secrecy and Society*, Maret describes a phenomenon outside the intelligence community that we find resonates equally well within it. In the context of the challenges of teaching secrecy (based on her work on government secrecy around environmental policy), Maret makes a useful distinction between information that is open, closed, or what she dubs as twilight.

The first two categories will be familiar to the intelligence professional. Open information is available to the public, and "it does not violate official secrets and is approved for public dissemination." Closed information is controlled by the institution and depends on a need to know; it "will either never be made public or become known decades later." Her third category is more intriguing: twilight information, she says, is the space between, "the half-knowing that results from redacted, declassified documents; while redaction suggests disclosure, openness, publicity, and transparency, it also contains uncertainty."

To extend Maret's analysis, the phenomenon of twilight information exists within the IC just as much as outside of it, whether in a nod to some proposition behind a compartment without disclosing the details, the unknown half-life of one's understanding after being read out of an old account, or a pack of lawyers heading to a closed-door meeting. These suggest there is a truth, and it is out there, but not here.

Informed Choice

In considering how the IC might reframe its relationship with secrecy and better contemplate costs, we looked at an unlikely source of inspiration: shopping.

In a traditional mental model of the intelligence cycle, the end user is someone remote to the process: an elected official, policymaker, soldier, etc. Yet in reality, intelligence practitioners are the principal consumers of intelligence, vastly outnumbering policymaking/decisionmaking consumers. As such, they exert a powerful collective force over what intelligence is targeted, collected, disseminated, analyzed, and evaluated. In essence, the internal IC consumer is the crucial intelligence sub-cycle—the sun gear within a planetary gearbox, if you will—in the traditional schematic of the intelligence cycle.

Over the years, intelligence organizations have tried to understand how intelligence practitioners value specific types of information, first through simple surveys (i.e., what users say is important) and in more recent years through data analytics (what users actually cite, download, share, etc.) These evaluations are useful to a point, but they do not require the user to account for carrying or epistemic costs. Furthermore, they measure what was used, but not what will be or should be used; they are neither predictive nor normative.

For practitioners, secrets are the ultimate free goods. They do not routinely consider the cost to acquire, use, ignore, store, or dispose. As with all (perceived) free goods, this leads to distortions in consumer behavior. Let's imagine that an intelligence analyst is writing an assessment based on two essentially identical pieces of information, one unclassified and one highly classified. The carrying costs of the unclassified information are *de minimus*, while the classified report would need to be safely handled and stored for 25–50 years, maybe more. The analyst, having no incentive to consider costs, relies on other factors in making their decision, such as perceived accuracy, reliability, exclusivity, or prestige.

Could intelligence practitioners rewire the secrecy heuristic? One option would be to explore strategies that increase the information available to the intelligence

consumer at what we might think of as the point of sale. Such strategies address what are known as information-market failures, i.e., when individuals or firms lack information about economic decisions because of ignorance, uncertainty, or inattention. The IC borrows terms from business and economics—client, customer, product, and so forth—but it lacks actual market mechanisms to inform consumers choices. Two long-running programs—Proposition 65 and Energy Star—offer a starting point for how the IC might change this model.

Proposition 65

In 1985, California lawmakers enacted the Safe Drinking Water and Toxic Enforcement Act, more widely known as Proposition (Prop) 65 after the original referendum, requiring that businesses provide clear and reasonable warnings to consumers when products contain substances that are known to cause cancer or reproductive harm. Prop 65 also banned the discharge of those substances into any source of drinking water.

Eventually Prop 65 became a national and even global phenomenon; each of us has encountered the now familiar warning that a particular item contains an ingredient known to cause cancer. Sometimes maligned as government overreach or used as a punchline for jokes about rats getting cancer, scholars of Prop 65 argue it has been extraordinarily successful in reducing toxic exposures to lead, ethylene oxide, perchloroethylene, and other substances, and in prompting significant reformulations of innumerable consumer products. For goods that cannot be reformulated, like seafood, Prop 65 has resulted in warnings about mercury that enables consumers to make informed choices. (Rechtschaffen, Willams)

EnergyGuide and ENERGY STAR

Another long-lived effort at informing consumer and producer choices can be found in the household appliance sector. In the wake of the energy crisis of the mid-1970s, the US government created the EnergyGuide labeling system that mandated that all products display a large label with detailed information about annual energy consumption and costs. In 1992, the Environmental Protection Agency established the ENERGY STAR certification program. Unlike the familiar yellow EnergyGuide label, the ENERGY STAR contains no information. Scholars note that regular updates to certification requirements are necessary as technology changes and new products come onto the market. (McWhinney, et al.)

Consumer surveys suggest these labeling schemes have an impact—known as a welfare effect—on retail purchase decisions, although the degrees vary. Scholars note that some consumers react more to detailed information in the EnergyGuide label or to the simpler ENERGY STAR certification; some will overpay (relative to projected cost savings); others will focus on expected operating costs versus efficiency or initial price. Still other consumers might disregard energy information altogether and focus on other aspects they value, like perceived prestige. These differences reflect the heterogeneity of purchasers that must be taken into account when designing information programs. Nonetheless, taken together, "the data suggest that the certification acts as a substitute for more accurate, but complex energy information."[a]

Objections

Could consumer-information systems help drive a dialogue among intelligence practitioners about which secrets to collect, evaluate, publish, and store? In turn, could individual decisions eventually scale to have collective impact, in essence setting a "price" for secrets, that might reshape the IC's approach? We think the answer to both questions is a qualified yes. That said, a brief discussion of objections is in order. At least three present themselves.

a. Sebastien Houde, "How Consumers Respond to Environmental Certification and the Value of Energy Information," E2e Working Paper 007 (December 12, 2016): 3.

The first objection is that we are am trying to commodify national security secrets, a category of goods that is not subject to market forces. In short, secrets aren't cans of tuna or dishwashers, and as such we cannot easily establish what economists refer to as a willingness to pay (WTP). We note that this exception is not as total as it might first appear. Markets do set WTP for goods and services that are similar to national security secrets, such as subscriptions for services that protect our personally identifying information on the web. This corollary only takes us so far, however, because there is no market to freely trade national security information. As the leading scholar in the field notes, "individual preferences, and aggregated WTP, may not capture the value of (some) goods."[a]

A second objection is that mechanisms like Prop 65 or EnergyGuide are intended to nudge consumers toward what should be, i.e., particular outcomes established by some third actor (such as state regulators), rather than what is. As such, even when the outcome might be widely considered to have a welfare effect—increasing organ donations, for example—the state is exercising influence over personal decisions or infringing personal choice. A discussion of debates within and about normative versus positive schools of economic thought is well beyond the scope of this article. It is sufficient for our purposes to acknowledge that objections in behavioral economics, social sciences, and popular media are likely to have parallels in intelligence that are not casually dismissed. All the same, these and other objections are a call to action rather than an argument for doing nothing.

Future Research Paths

That begins with the IC, which excels at understanding foreign trends and adversaries but spends less time trying to understand itself. How might we address the knowledge gaps?

- Applied ethnographic research blending qualitative and quantitative approaches, including observation, interviews, surveys, and data collection, could shed light on why, when, and how practitioners collect, evaluate, and share individual reports.
- Web analytics could tell us how information flows into, through, and out of IC components.
- Gaming could sharpen our understanding of when and why collectors, analysts, and customers under or over value intelligence reporting and how price sensitive they are.
- Artificial intelligence might provide deeper insights into the IC's vast information holdings, refine new information needs, discover alternative data, and reduce the inevitable tailings.

Taken together, these and other avenues of research could help animate a debate within the IC about how to evaluate and reduce the epistemic and carrying costs of secrecy.■

a. Cass R. Sunstein, "Five Objections to Commodification" (March 2, 2026). https://ssrn.com/abstract=6329338 or http://dx.doi.org/10.2139/ssrn.6329338.

Select Bibliography

Ben Jaffel, Hager, and Alvina Hoffmann, Oliver Kearns, Sebastian Larsson, "Collective Discussion: Toward Critical Approaches to Intelligence as a Social Phenomenon," *International Political Sociology* (2020) 14, 323–44.

Bilmes, Linda J., "Current and Projected Future Costs of Caring for Veterans of the Iraq and Afghanistan Wars," *M-RCBG Faculty Working Paper No. 2011-06* (2011).

Bilmes, "The Long-Term Costs of United States Care for Veterans of the Afghanistan and Iraq Wars," Costs of War Project, Brown University, Watson Institute of International & Public Affairs, August 18, 2021.

Bok, Sissela, *Secrets: On the Ethics of Concealment and Revelation*, (Pantheon Books, 1982).

Brown, Zachery Tyson, "Biden Has a Golden Chance To Remake US Intelligence," *Foreign Policy*, January 22, 2021
Connelly, Matthew, *The Declassification Engine* (Pantheon, 2023).
Coulthart, Stephan, and Abebe Rorissa, "Growth, Diversification, and Disconnection: An Analysis of 70 Years of Intelligence Scholarship," *Intelligence and National Security* 38, No. 1 (June 2023): 1–17.
Fabre, Cecile *Spying Through a Glass Darkly: The Ethics of Espionage and Counter-intelligence* (Oxford University Press, 2022)
Garton Ash, Timothy, *The File: A Personal History* (Random House, 1997).
Hathaway, Oona "Keeping the Wrong Secrets: How Washington Misses the Real Security Threat," *Foreign Affairs* (January/February 2022).
Hatlebrekke, Kjetil Anders, *The Problem of Secret Intelligence* (Edinburgh University Press, 2019).
Hegghammer, Thomas, "The War on Terror Supercharged State Power," *Foreign Affairs* (September/October 2021).
Hofstadter, Richard, "The Paranoid Style in American Politics," *Harper's Magazine* (November 1964).
Houde, Sebastien, "Consumers' Response to Quality Disclosure and Certification: An Application to Energy Labels," E2e Working Paper 007 (December 2016).
Lathrop, Charles, ed., *The Literary Spy* (Yale University Press, 2004).
Lebovic, Sam, *State of Silence: The Espionage Act and the Rise of America's Secrecy Regime* (Basic Books, 2023).
LeCompte, Margaret, and Jean Schensul, *Designing and Conducting Ethnographic Research*, Vol. 1 (AltaMira Press, 1999).
Lester, Genevieve, *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence* (Cambridge University Press, 2015).
Mahnken, Thomas G., Selective Disclosure: A Strategic Approach to Long-Term Competition (Center for Strategic and Budgetary Assessments, 2020).
Maret, Susan, "Concealing in the Public Interest, or Why We Must Teach Secrecy," *Secrecy and Society* 2, No. 2 (January 2021).
Marrin, Stephen, "Analytic Objectivity and Science: Evaluating the US Intelligence Community's Approach to Applied Epistemology," *Intelligence and National Security* 35, No. 3 (2019).
Manosevitz, Jason, review of Genevieve Lester, *When Should State Secrets Stay Secret? Accountability, Democratic Governance, and Intelligence* (Cambridge University Press, 2015), *Studies in Intelligence* 60, No. 3 (September 2016).
Miller, Bowman, "The Death of Secrecy: Need To Know…With Whom To Share," *Studies in Intelligence 55*, No. 3 (September 2011).
Monyihan, Daniel Patrick, *Secrecy: The American Experience* (Yale University Press, 1998).
Pfaff, Debora and Bowman Miller, "From a Whisper to a Shout: The IC Should Use Its Outside Voice," *Research Short* (National Intelligence University, June 23, 2021).
Pozen, David, "The Leaky Leviathan," *Harvard Law Review* 127, No. 512 (2013).
Rechtschaffen, Clifford, and Patrick Williams, "The Continued Success of Proposition 65 in Reducing Toxic Exposures," *ELR News & Analysis* (December 2005).
Sawyer, Ralph, "Traditional Chinese Conceptions and Approaches to Secrecy, Denial, and Obfuscation," *Studies in Intelligence* 64, No. 1 (March 2020).
Schklar, Judith, "The Liberalism of Fear," in *Liberalism and the Moral Life*, (Harvard University Press, 1989).
Shils, Edward, *The Torment of Secrecy The Background and Consequences of American Security Policy* (The Free Press, 1956).
Sissel, Georg, "The Sociology of Secrecy and of Secret Societies," *American Journal of Sociology* 11, No. 4 (January 1906).
Stolze, Travis D., review of Matthew Connoly, *The Declassification Engine* (Pantheon, 2023), *Studies in Intelligence* 67, No. 2 (June 2023).
Spivack, Miranda S., *Backroom Deals in Our Backyard: How Government Secrecy Harms Our Communities and the Local Heroes Fighting Back* (The New Press, 2025).
Sturm, Brian, and Renee Bosman, Sylvia Leigh Lambert, "Windows and Mirrors: Secret Spaces in Children's Literature," *New Review of Children's Literature and Librarianship* 14, No. 2 (2008).
Travers, Mark, and Leaf Van Boven, Charles Judd, "The Secrecy Heuristic: Inferring Quality From Secrecy in Foreign Policy Contexts," *Political Psychology* (2013).
Tzamarelou, Sofia, *Intelligence in Democratic Transitions: A Comparative Analysis of Portugal, Greece, and Space* (Georgetown University Press, 2024).
Ypi, Lea, *Free: A Child and a Country at the End of History* (W.W. Norton & Co., 2021).
Weinbaum, Cortney, and Bradley Knopp, Soo Kim, Yuliya Shokh, *Options for Strengthen All-Source Intelligence: Substantive Change Is Within Reach* (RAND Corporation, 2022).
Whitesmith, Martha, "Justified true belief theory for intelligence analysis," *Intelligence and National Security* 37, No. 6 (2022).■