Secrecy and Intelligence: Introduction

Kathleen Vogel
University of Maryland, kvogel12@umd.edu

Brian Balmer
University College London, b.balmer@ucl.ac.uk

Secrecy and Intelligence: Introduction

Abstract

The catalyst for this special issue of *Secrecy and Society* stems from a workshop titled "Secrecy and Intelligence: Opening the Black Box" at North Carolina State University, April, 2016. This workshop brought together interested scholars, intelligence practitioners, and civil society members from the United States and Europe to discuss how different facets of secrecy and other practices shape the production of knowledge in intelligence work. This dialogue aimed to be reflective on how the closed social worlds of intelligence shape what intelligence actors and intelligence analysts, who include those within the intelligence establishment and those on the outside, know about security threats and the practice of intelligence. The papers in this special issue reflect conversations that occurred during and after the workshop.

Secrecy and Intelligence: Introduction

Kathleen M. Vogel[1] and Brian Balmer[2]

Abstract
The catalyst for this special issue of *Secrecy and Society* stems from a workshop titled "Secrecy and Intelligence: Opening the Black Box" at North Carolina State University, April, 2016. This workshop brought together interested scholars, intelligence practitioners, and civil society members from the United States and Europe to discuss how different facets of secrecy and other practices shape the production of knowledge in intelligence work. This dialogue aimed to be reflective on how the closed social worlds of intelligence shape what intelligence actors and intelligence analysts, who include those within the intelligence establishment and those on the outside, know about security threats and the practice of intelligence. The papers in this special issue reflect conversations that occurred during and after the workshop.

In her inaugural editorial for this journal, Susan Maret (2016) convincingly argues that secrecy should be treated as both a social problem and a wicked problem. It is a problematic condition that demands action; it is complex and exceedingly difficult to resolve. This

---

1   Associate Professor, School of Public Policy, University of Maryland at College Park.
2   Professor, Department of Science and Technology Studies, University College London.

special edition on *Secrecy and Intelligence* introduces two further dimensions for characterising secrecy. Reflecting the guest editors' shared background in Science and Technology Studies (STS), we would characterise secrecy as a profoundly epistemic problem. Moreover, for all scholars of secrecy, we suggest secrecy presents itself as a difficult methodological problem.

The epistemic problem of secrecy is easily stated: Secrets are knowledge, and secrecy fundamentally involves asymmetries in knowledge. For a secret to exist, someone (or something, if we want to extend our analysis to computers, "secrets of the universe," or other such entities) has to know that secret, and others must be excluded from that knowledge. Indeed, historian Peter Galison has argued that secrecy, as the removal of knowledge, should be described as anti-epistemology, although this belies the fact that, though hidden, someone still is in possession of the concealed knowledge (Galison 2004). And, for them, secrecy remains a matter of epistemology.

Secrecy, however, is about far more than disembodied knowledge sitting in some people's heads and not in others. When secrets are produced, maintained, and revealed, they have multiple facets, including an ethics, a geography, a sociology, and a history.[3] The ethics of secrecy, as explored in the classic study by Sissela Bok

---

[3] This list is not intended to be exhaustive. One can imagine fruitful potential for studies of the political economic, socio-legal, and anthropological dimensions of secrecy, and so on.

(1989), takes an explicitly normative approach and asks: When is it right to keep or reveal secrets? Indeed, this is probably the most familiar way in which academics have tackled the issue of secrecy.

But secrecy also has a significant geographical element. It might seem trivial to state that secrecy takes place somewhere. But, as geographer Trevor Paglen points out, this statement draws attention to the materiality of secrets as a key reason why they generate paradoxes and contradictions:

> Secret relations, programs, sites, and events have to be made out of the same 'stuff' that everything else (the nonsecret world) is made of. Because there are no such things as invisible factories, airplanes made out of unearthly ghost-matter...logics of secrecy are contradicted by their material implementations. (Paglen 2010, 760)

For Paglen, the very effort of people trying to make and keep secrets, by getting things and people to behave "as if" they were invisible or intangible, will always be betrayed by the plain fact that they are not so. Of significance for scholars of secrecy, this work and effort of creating and maintaining the secret in the face of such internal tensions is itself open to empirical social scientific investigation. Rather than focussing solely on the normative questions, which are of course important, Paglen's claims shift analytical focus to the social processes and dynamics of secrecy. We can ask: How does secrecy operate, and what are the consequences of that secrecy?

These discussions of secrecy are central to discussions of intelligence and how knowledge is produced within and by intelligence communities. This special issue takes a special look at the often fraught relationship of secrecy, transparency, and intelligence. We do this through close engagement with individuals who have either spent time working within the intelligence community, or who have spent time closely researching and analysing these secret communities. We were motivated to create this special issue based on a series of events in the United States and the United Kingdom that have allowed us to open up the "black box" of intelligence at this opportune time.

Significantly, a major impetus came from within the usually closed world of the U.S. Intelligence community. With the noted intelligence failures prior to the September 11th attacks and the 2003 Iraq War (National Commission on Terrorist Attacks Upon the United States 2004; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction 2005), the U.S. intelligence community has recognized the need to acquire new outside expertise to mitigate future intelligence failures. In 2008, the Office of the Director of National Intelligence issued Intelligence Community Directive Number 205, "Analytic Outreach," which charges intelligence analysts to "leverage outside expertise as part of their work…[and]…explore ideas and alternative perspectives, gain new

insights, generate new knowledge, or obtain new information" (Office of the Director of National Intelligence 2008). The Directive recognizes the importance for analysts to move out of their classified domains in order to tap into valuable outside knowledge and expertise relevant to intelligence problems, and that can challenge the erroneous group-think that can occur in the closed worlds of intelligence. Furthermore, a collection of current and former intelligence practitioners have published articles discussing facets of knowledge production in intelligence and how this kind of inquiry can suggest improvements for intelligence collection, analysis, and policymaking (Fingar 2011; George and Bruce 2008; Miller 2008; Treverton 2008; Kerr et al. 2005; Johnston 2005; Rieber and Thomason 2005).

The WikiLeaks and Snowden affair have made more apparent the vast scale and scope of the U.S. intelligence industrial complex (Macaksill and Dance 2013; Priest and Arkin 2012). Snowden has also attracted academic interest from scholars in the relationship between secrecy and forms on non-knowledge, such as ignorance (Rappert and Balmer 2015a). The Snowden revelations, in particular, have drawn back the shroud on U.S. intelligence for public scrutiny, and raised troubling questions about what these secret communities are doing and what levels of oversight are needed for how these communities produce knowledge.

To take advantage of this unique moment - and what served as the catalyst for this special issue - we organized a workshop in April 2016 called "Secrecy and Intelligence: Opening the Black Box" at North Carolina State University.[4] This workshop brought together interested scholars, intelligence practitioners, and civil society members from the United States and Europe to discuss how different facets of secrecy and other practices shape the production of knowledge in intelligence work. This dialogue aimed to be reflective on how the closed social worlds of intelligence shape what intelligence actors and intelligence analysts, who include those within the intelligence establishment and those on the outside, know about security threats and the practice of intelligence. We were motivated to engage with practitioners in both the U.K. and U.S. intelligence communities in this context, out of curiosity regarding its function as an analytic object of study, to learn what such encounters can tell us about this secret community and how it produces security knowledge, and to observe and document the effects of intelligence on S&TS and public spheres (Vogel and Dennis 2018).

In addition to the paper presentations at the workshop (some of which are presented in expanded form here), there was also the

---

4 The workshop was funded by the National Science Foundation, the Defense Intelligence Agency Intelligence Community Center for Academic Excellence (IC-CAE), the Laboratory for Analytic Sciences, the Kenan Institute for Engineering, Technology, and Science, the Buchdahl Lecture Fund [], and NC State.

opportunity for participants to "witness" the workings of a real-life intelligence research laboratory as part of the workshop activities. The National Security Agency's Laboratory for Analytic Sciences (LAS), located at NC State, agreed to open its doors to our workshop participants. The LAS is a big data research center that aims to produce technology and tradecraft to improve intelligence analysis for the future.[5] This opportunity provided a rare moment to witness the tensions between secrecy and transparency - and the awkward encounters of how members of the U.S. intelligence community and the workshop participants tried to navigate these terrains.

For U.S. citizens at the workshop, the LAS organized a tour of the sensitive compartmented information facility (SCIF), which was the classified space on the NC State campus in which NSA analysts could work. To obtain access to the SCIF, each person was required to submit their name, date of birth, and social security information so that a background check could be run. Non-U.S. citizens were not allowed into the SCIF but were given the opportunity to see demos of some of the unclassified technology prototypes, offsite in classrooms on the NC State campus, that were being developed by the LAS. What was interesting, and reflective of the spirit of the workshop, was the ironic and unexpected encounter of secrecy and transparency during the tour and demos. The U.S. citizens who were allowed access into

---

5   At https://ncsu-las.org/

the SCIF - the seeming "crown jewels" of the LAS enterprise - felt that they were given long and drawn-out canned PowerPoint lectures about LAS, with very little time to tour the facility and ask open-ended questions about the work done there. This was certainly not deliberate. Although the LAS leadership felt they were being very transparent by letting members of the uncleared public into the SCIF (at that time, there had not been such a large group of the public allowed into the LAS SCIF) and providing background information on the lab, this was not perceived by the U.S. participants. In contrast, the foreign participants at the workshop felt they received a lot of information, openness, and transparency about the technological tools being developed at LAS, as they were able to see and touch the demos (held in campus rooms outside of SCIF), and found them to include a very worthwhile set of presentations - this even though the foreigners were shunned from visiting the SCIF. We recount this anecdote not to criticise the lab; rather, these experiences reveal the interesting and often contradictory tensions that exist within notions of secrecy and transparency in matters of intelligence.

As a small reminder from this encounter, and from our years of research involving interviews with intelligence practitioners and historical research on formerly classified national security materials, we have become sensitized to the disconnects among academic,

intelligence, and civil society communities, and the need for more substantive and extended discussions among them to better understand the production of knowledge in intelligence, and how the work and sustained interactions from these disparate communities can beneficially inform one another. Beyond the workshop, we hope this special issue is one way forward to create a constructive space for this kind of dialogue and engagement to continue.

The series of papers in this volume speak to a variety of facets of secrecy (and its twin, transparency), and how they operate within and across different facets of intelligence activities, programs, agendas, and agencies.

The history of secrecy is equally pertinent to our special edition, with a number of contributors reflecting on their contribution to the historiography of intelligence. It is important here to understand secrecy as a phenomenon that changes over time. As such, historian Alex Wellerstein has argued that although all societies experience secrecy in some form or another, the organization of secrecy (and transparency) and the targets of concern around secrets are products of historical context. Placing the origins of contemporary manifestations of U.S. concerns about secrets as far back as WWI, he claims:

> American secrecy is relatively new (early-to-mid 20th century forward)… it had a few definite points of beginning, that the

assumption that the world was full of increasingly dangerous *information* that needed government regulation was not a timeless one, and that it had *changed* over time in a variety of distinct and important ways. (Wellerstein 2016)

Approaching these different facets of secrecy and society raises adjunct issues around methodology and researching secrecy. In thinking through the most appropriate ways to investigate secrecy, there is an overarching question about whether research on secrets is different in degree or kind from other topics of social research (e.g., Rappert and Balmer 2007, 2015a, 2015b). On the one hand, resolving problems of access, trust, veracity, and interpretation are pervasive across many forms of social research and are featured in any good methods textbook. It remains an open question as to whether research into secrets demands fundamentally different approaches. It is clear that the problems listed above are exacerbated in situations in which secrecy is endemic, institutionally embedded, and even part of the *raison d'etre* of the organisation, group, or individual being studied. It is worth noting here that several contributions to this volume are personal reflections on researching secrecy and intelligence, rather than traditional academic articles reporting research results (see Goodman, Nolan, and Räsänen). We regard these contributions as providing crucial preliminary steps to building a more systematic and rigorous methodological literature on this topic.

In this collection, three historians – Goodman, Macrakis, and Walton - reflect on their research into the secret world of intelligence. Each has a different experience of accessing sources, ranging from Goodman - writing an official history of the UK Joint Intelligence Committee and therefore with what he calls "unparalleled access" - to Walton - relying on newly declassified documents - and Macrakis, who used both oral history and archival analysis to understand the history of intelligence. Even Goodman, who had the most access, raises the "equal and opposite" problem of having too much information to sift through. He also points out that having such access poses questions about credibility; readers of his work need to be in a position to trust his account based on documents that cannot be checked independently. So, rather than a simple polarisation between concealment and revelation, even writing about secrecy creates asymmetries of knowledge that, *prima facie*, a historical account aims to dissolve.

All three historians raise a different issue linked to earlier discussion of the geography of secrecy. None was uncovering a single secret locked in a safe somewhere. Macrakis notes the long, slow process involved in piecing together different archival and oral sources, with the best material not necessarily where it was expected to be. Goodman notes that the record of the Joint Intelligence

Committee consists of years of paperwork in different formats: minutes, memoranda, confidential annexes, tactical assessments, and suchlike. Echoing Paglen's point about the materiality of secrecy creating contradictions, Walton notes how a "mislaid" archive of 8,000 files, taking up 15 miles of shelving, on colonial Kenya could not remain lost (short of being destroyed). Local residents near the archive even referred to the site as "spook central."

Some of the papers also examine the larger macro-level political context and the larger political forces that support and sustain, as well as attempt to subvert, secrecy and transparency within intelligence. Miles follows the unresolved U.S. political debate about whether to continue to classify or disclose more details about the U.S. intelligence budget; supporters and critics both deploy arguments involving the U.S. Constitution, the need for public accountability, and security to rationalize their positions - the debates over secrecy and transparency in U.S. intelligence have a longstanding, and unresolved, political rhetoric behind them dating back to the 1970s. Beyond disclosing top-line intelligence budget figures, the U.S. Congress continues to wrestle with whether to disclose more intelligence budget information as a way to strengthen and support U.S. intelligence, or whether this will introduce dangerous threats to U.S. national security.

In contrast to Miles, where the political debate over the U.S. intelligence budget remains stalled, McDermott's article shows how such debate can be ruptured - by outsiders such as Edward Snowden, the media, and other civil society actors working through public disclosures and FOIA litigation. McDermott painstakingly details how, since September 11, 2001, the U.S. intelligence community has been able to obtain intelligence from emails, text, video chats, and photographs on potential U.S. national security threats through a variety of technologically mediated means - for example, servers of U.S. companies such as Microsoft, Yahoo, Skype, Google, and Facebook. This data has been enabled by a series of secret U.S. courts (whose data and decisions are classified and not open to public scrutiny), and who become the ultimate arbiter on what is allowable for surveillance by U.S. intelligence. McDermott argues that the obligation of these courts and members of the U.S. intelligence community to protect intelligence sources, methods, and activities - without a clear legal definition of methods - allows for the intelligence community to create broad swaths of boundaries around what is withheld from public purview. However, McDermott notes that this very practice of expanding the boundaries of what is considered to be classified is recognized as being contrary to building public trust in intelligence, which is seen as essential to mission success. The

protective features of transparency seem to be irreconcilable with the inherent tendency by U.S. intelligence to classify sources and methods.

Albro's article examines the problem of information secrecy by unpacking the opacity of "black box," algorithm-based, big-data tools that are being developed by certain U.S. intelligence agencies to study and anticipate the behavior of foreign cultures that are of concern to U.S. national security. Albro argues that these technological tools are creating new regimes of secrecy that are obscuring the collection process from analysts; this opacity increases the risk of data distortion and analysts thereby fundamentally misunderstanding the behavior of cultural groups, which can lead to poor national security assessments and policymaking.

Writing from the personal perspective of serving as a former intelligence practitioner and simultaneously as sociology graduate student conducting an ethnography of an intelligence agency, Nolan advances the idea of "boundary personnel" - people who navigate between the worlds of academia and national security - and how they provide value added in revealing the unique facets of tacit knowledge that encompasses intelligence work that outside researchers would not be able to access. At the same time, Nolan documents the inherent challenges facing such boundary workers and how the secrecy that

surrounds intelligence work even permeates the mundane aspects of work life, at times creating social distance among its employees, creating new forms of invisible labor to maintain secrecy, and producing distorting effects on the work - not only as a practitioner, but also as a research ethnographer. Nolan makes the case for the need for more of these boundary personnel within intelligence organizations, so we can better understand how these complex centers of power and knowledge production operate.

In a similar vein, Räsänen offers a methodological reflection on her qualitative fieldwork within the Swedish intelligence community as a form of collaboration. Unlike some traditional ethnographies in which the researcher is a distanced observer of the ethnographic site, Räsänen worked in partnership with the organisation with the explicit aim of bringing about change. As she notes: "Practitioners learn about the research process as the researchers learn about the practitioners' work practices. Rather than just passing over information to the researcher, the practitioner works with them in knowledge generation." Such co-production also meant that the object of research itself changed over the course of the fieldwork as a direct result of carrying out the research. As with Nolan, this type of subject-researcher relationship is not without challenges – not least in how the researcher maintains some critical distance - but Räsänen concludes

that, on balance, the time and energy expended was beneficial to both the practitioners and the academic researchers.

This project advances knowledge in the field of secrecy studies, science and technology studies, and related disciplines by examining the different geographies and practices of knowledge in the secret worlds of intelligence, and how to study them using different analytic methodologies and ethical sensibilities. As we see signs that the previously closed worlds of intelligence are becoming at least slightly more open, we hope that this special issue is just the start of more dialogues around these topics.

References

Aradau, Claudia. 2017. "Assembling (non)Knowledge: Security, Law, and Surveillance in a Digital World." *International Political Sociology* 11, no. 4: 327-42. https://academic.oup.com/ips/article/doi/10.1093/ips/olx019/4372386

Bok, Sissela. 1989. *Secrets: On the ethics of concealment and revelation.* New York: Vintage.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. 2005. *Report to the President.* March 31. Washington, DC: Supt. of Docs., U.S. G.P.O. https://fas.org/irp/offdocs/wmdcomm.html

Fingar, Thomas. 2011. *Reducing Uncertainty: Intelligence Analysis and National Security*. Palo Alto, CA: Stanford University Press.

Galison, Peter. 2004. "Removing Knowledge." *Critical Inquiry* 31, no. 1: 229-43. https://dash.harvard.edu/bitstream/handle/1/2580255/removing%20knowledge.pdf?sequence=2

George, Roger Z., and James B. Bruce, eds. 2008. *Analyzing Intelligence: Origins, Obstacles, and Innovations.* Washington, DC: Georgetown University Press.

Johnston, Rob. 2005. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study.* Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency. http://www.dtic.mil/dtic/tr/fulltext/u2/a507369.pdf

Kerr, Richard, Thomas Wolfe, Rebecca Donegan, and Aris Pappas. 2005. "Collection and Analysis on Iraq: Issues for the Intelligence Community." *Studies in Intelligence* 49, no. 3: 47-54.

Macaksill, Ewen, and Gabriel Dance. 2013. "NSA Files: Decoded: What the Revelations Mean for You." *Guardian,* November 1. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1

Maret, Susan. 2016. "The Charm of Secrecy: Secrecy and Society as Secrecy Studies." *Secrecy and Society* 1, no. 1: 1-28. http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1014&context=secrecyandsociety

Miller, Bowman H. 2008. "Improving All-Source Intelligence Analysis: Elevate Knowledge in the Equation." *International Journal of Intelligence and Counterintelligence* 21, no. 2: 337-54.

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report: Final report of the National Commission on Terrorist Attacks Upon the United States.*

Washington, DC: Supt. of Docs., U.S. GPO. https://www.9-11commission.gov/report/911Report.pdf

Office of the Director of National Intelligence. 2008. *Intelligence Community Directive 205: Analytic Outreach.* July 16. http://www.ncix.gov/publications/policy/docs/ICD_205-Analytic_Outreach.pdf

Paglen, Trevor. 2010. "Goatsucker: Towards a Spatial Theory of State Secrecy." *Environment and Planning D: Society and Space* 28, no. 5 (January online, October print): 759-71. https://doi.org/10.1068/d5308

Priest, Dana, and William A. Arkin. 2012. *Top Secret America: The Rise of the New American Security State,* New York: Little Brown & Company.

Rappert, Brian, and Brian Balmer. 2007. "Rethinking 'Secrecy' and 'Disclosure.'" In *Technology and Security: Governing Threats in the New Millenium*, edited by Brian Rappert, 45-65. Basingstoke, UK: Palgrave.

Rappert, Brian, and Brian Balmer. 2015a. "Ignorance is Strength? Intelligence, Security and National Secrets." In *Routledge International Handbook of Ignorance Studies,* edited by Matthias Gross and Linsey McGoey, 328-337. London: Routledge.

Rappert, Brian, and Brian Balmer, eds. 2015b. *Absence in Science, Security and Policy: From Research Agendas to Global Strategy*. Basingstoke, UK: Palgrave MacMillan.

Rieber, Steven, and Neil Thomason. 2005. "Creation of a National Institute for Analytic Methods." *Studies in Intelligence* 49, no. 4: 71-78.

Treverton, Gregory F. 2008. *Assessing the Tradecraft of Intelligence Analysis*. Santa Monica, CA: RAND Corporation.

Vogel, Kathleen M., and Michael A. Dennis. 2018. "Tacit Knowledge, Secrecy, and Intelligence Assessments: STS Interventions by Two Participant-Observers." *Science, Technology, and Human Values* 43: 1-30.

Wellerstein, Alex, ed. 2016. "My conversation on secrecy with a Super Spook." *Restricted Data: The Nuclear Secrecy* (blog), March 18. http://blog.nuclearsecrecy.com/2016/03/18/conversation-with-a-super-spook/