REVIEW ESSAY

Truth Telling, Trust, and Just Intelligence Theory

Shannon Brandt Ford

Spies, Lies, and Algorithms: The History and Future of American Intelligence, by Amy B. Zegart (Princeton, N.J.: Princeton University Press, 2023), 424 pp., cloth $55, paperback $21.95, eBook $21.95.

The Ethics of National Security Intelligence Institutions: Theory and Applications, by Adam Henschke, Seumas Miller, Andrew Alexandra, Patrick F. Walsh, and Roger Bradbury (London: Routledge, 2024), 288 pp., cloth $152, eBook open access on Taylor & Francis website.

Big Data, Emerging Technologies and Intelligence: National Security Disrupted, by Miah Hammond-Errey (London: Routledge, 2024), 212 pp., cloth $152, eBook $31.99.

The function of spying has always been present in political life as a widespread practice for mitigating against threats (think of Moses sending out spies to scout the land of Canaan or the Roman army's use of *speculatores* and *exploratores* for scouting and reconnaissance). But the notion that intelligence should exist as a set of permanent institutions, with ongoing responsibilities for maintaining the national security of the state, is a relatively recent innovation.[1] This review essay examines the ethics and moral purpose of these national security intelligence institutions, putting into conversation three recent works on the topic. In *The Ethics of National Security Intelligence Institutions*, Adam Henschke, Seumas Miller, Andrew Alexandra, Patrick Walsh, and Roger Bradbury

Shannon Ford, Curtin University, Perth, Australia (shannon.ford@curtin.edu.au)

Ethics & International Affairs, 39, no. 1 (2025), pp. 89–101.

doi:10.1017/S089267942510004X

examine the ways that liberal democracies have come to rely on intelligence institutions for effective decision-making, and they look at the best ways to limit these institutions' power and constrain the abuses they have the potential to cause. Their goal is to construct applied ethical theory in the specific context of intelligence institutions.

In contrast, the other two monographs are not at all concerned with ethical theory. Instead, their goal is to look behind the curtain and derive an insight into the current beliefs of intelligence practitioners. In particular, what do practitioners think is the purpose of the intelligence institutions of which they are a part? And what role do they believe ethics plays in their work? Miah Hammond-Errey's *Big Data, Emerging Technologies and Intelligence* sets out to show how big data is transforming what intelligence is, how it is practiced, and the relationships intelligence institutions have with society. She has one chapter specifically titled "Ethics and Bias," but most of her other chapters also address ethical themes for big data and intelligence, such as new social harms, privacy, trust, transparency, and legitimacy. Amy Zegart's *Spies, Lies, and Algorithms* argues that American intelligence institutions require dramatic change to harness new technologies faster and more effectively than their adversaries. Through analysis of her interviews with senior U.S. intelligence officials, Zegart concludes that intelligence officers "think about ethics a lot." In other words, intelligence officers are aware that they work in a profession filled with ethical dilemmas and that moral decision-making is an important part of the job.

In this review essay, I explore some of the key ethical themes that appear consistently across the works under consideration. I start out, first of all, by highlighting that all three books agree that new technologies are having a significant impact on the business of intelligence and, consequently, the types of ethical dilemmas now confronting intelligence practitioners. Henschke and colleagues' text is the one that most directly contributes to recent debates about intelligence ethics.[2] The novelty of their approach, as we will see, is to apply ethical theory in the context of intelligence institutions. In contrast, Zegart and Hammond-Errey seek to draw out the thoughts and beliefs of intelligence practitioners about their work. It turns out that many of these thoughts and beliefs have ethical content. Next, I look at the tension created by the institutionalization of intelligence with liberal-democratic norms and values. The ethical challenge for intelligence institutions in

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

liberal democracies is how to do their job effectively in a way that is privacy respecting. Then, I examine the argument that the fundamental moral purpose of intelligence institutions should be truth telling; that is, the assumption that effective intelligence is an epistemic activity that improves decision-makers' understanding of the world such that they are enabled to make better decisions. As it turns out, many practitioners agree on this point. Finally, I examine what each book has to say about the notion that intelligence institutions should actively seek ways to maintain the trust of the public despite their activities being shrouded in secrecy.

New Technologies and Ethical Dilemmas

A key theme highlighted across all three books is the way in which new technologies are having a significant impact on the business of intelligence and the types of ethical dilemmas now confronting intelligence practitioners. For instance, Henschke and colleagues discuss how changes in information and communication technologies are fundamentally changing intelligence (p. 200). They argue that disruptive technologies such as facial recognition, the ease of access to encryption, and the rise of open-source intelligence require a "principled and reflective approach" for intelligence institutions to adapt effectively, with a particular focus on accountability. Importantly, a straightforward application of just war principles, they believe, is insufficient to meet the current (and future) technology challenges (p. 186). More on this below.

Zegart argues in her book that rapid change in technologies has made intelligence information harder to understand. She describes how constant cyberattacks, for instance, compromise trust in information and computer systems. Being able to trust computer systems to work reliably is essential for modern society to function (p. 269). Furthermore, in cyber conflict, the variety of weapons is more important than the quantity. The intelligence demands are high because variety requires identifying more and more vulnerabilities and ways to exploit them (p. 273). An important implication for the United States is that this technological change has not been accompanied by an improvement of congressional oversight, and congressional institutions remain poorly equipped to oversee and regulate intelligence challenges, including the inevitable ethical dilemmas they create (p. 224).

Hammond-Errey focuses specifically on how big data is transforming intelligence and highlights the key impacts on ethical considerations for intelligence.

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

These considerations include both the collection of information and secret intelligence, as well as the analytical processes used to create intelligence products to inform decision-making (p. 2). Participants in Hammond-Errey's study described the abundance of data about individuals as a profound change for intelligence agencies because there is now a record of almost all human activities that can be traced to the individual level (p. 25). For example, one participant said that "now, we can build up a profile of an individual to a fairly detailed level, provided we have the right data and the right analytics to run over it" (p. 29). Another participant said: "Fundamentally the impact of big data [on intelligence] is about understanding purpose … Why are we doing this? … People are trading off their civil liberties because that's what is happening. You're giving something up to prevent a worse thing happening over here" (p. 139).

In thinking about how to respond to the complex and rapidly changing ethical challenges facing intelligence institutions, Henschke and colleagues have developed a novel and pragmatic approach in *The Ethics of National Security Intelligence Institutions*.[3] They suggest that like the conventional just war tradition (JWT) holds that exceptional moral rules apply in warfare, something similar applies to intelligence.[4] They are not the first to discuss intelligence ethics.[5] What is novel about their work compared to, say, someone like Cécile Fabre's,[6] is their specific focus on the key role played by the institutions themselves. In other words, intelligence institutions have a key role to play in determining the ethical framework within which intelligence practitioners operate.

Henschke argues, in one of his solo-authored chapters in the volume, that because intelligence "consists of lying and manipulating people and damaging and destroying the truth—the specific rules for conduct in intelligence … must be radically different in content from the specific standards for conduct in ordinary life" (p. 56). But rather than taking the principles of just war and applying them directly to intelligence, Henschke is of the school of thought that bespoke ethical principles for just intelligence theory (JIT) should be developed instead (p. 52). For instance, he argues that the intelligence equivalent of the JWT *ad bellum* requirement is *jus ad intelligentiam.* These are the high-level considerations about wide-scale intelligence operations and the basic conditions around the use and existence of intelligence institutions (p. 60). He then suggests that the just cause principle applied to intelligence says that the national security intelligence agencies of political community *A* are justified in intelligence activities against actor *B* if, and only if, *A*'s purpose is to enable decision-making that protects against any

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

national security threat posed by *B* and/or to enable decision-making that gives it a competitive national security advantage relative to *B* (p. 60). Henschke and his colleagues are not the first to attempt adapting just war principles to conflicts other than war.[7] Nor are they the first to suggest developing just intelligence principles based on the just war tradition.[8] But the argument that intelligence institutions themselves play a determinative role in the formation of JIT is a novel and underdeveloped approach to the issue.

The other thing about the JIT adaptations by Henschke and colleagues is that they are generally convincing. In particular, their conclusion that an entirely new moral principle should be added to JIT—that is, the risk of transparency principle (ROT)—is, in my opinion, correct. This principle says that "any intelligence institution, or institutional actor using intelligence, should act in such a way that should those actions be made public, they will not undermine the justificatory purpose of the action" (p. 223). In other words, an intelligence practitioner faced with an ethical dilemma should assume that their decision will sooner or later become public knowledge and that any morally unjustifiable action that becomes publicly known will damage trust in the institution. Intelligence actors and agencies need to be trusted by the citizens and decision-makers that they are working for, and in whose name they derive their moral legitimacy (p. 223).[9]

What is particularly noteworthy in the present is how well the ROT principle resonates with intelligence practitioners. Many intelligence officers told Zegart, for instance, that their guide for grappling with ethical dilemmas is imagining what the American public would think if the secret was public. As one put it, "Would I be proud to tell the American people that we did that?" (p. 97). In addition, Hammond-Errey makes the point that a key impact of the big data landscape is that very little is likely to remain secret forever (p. 46). One of Hammond-Errey's interlocutors, former Principal Deputy Director of National Intelligence Sue Gordon, said that "I think the disclosures by Edward Snowden were really significant [as they] broke open this idea that there were intelligence activities going on broadly about which the American people and our allies and partners had opinions. Then you have 2016, the Russian interference in our election, and we have to reveal that because it's the American people that are being affected…I think it's just this movement of recognition that you have to be able to share some of the information to the people that are being affected in order to engender trust…" (p. 46).

In contrast, their proposed JIT equivalent for last resort—logical resort for intelligence (LRI)—is less convincing. This says that as awareness of a potential

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

national security threat increases, more intelligence operations that serve national security are permitted (p. 64). The rationale for rejecting last resort as a JIT principle is that intelligence is an ongoing national security practice that precedes war and so by definition cannot be a last resort (p. 63). But there is also a sense in which intelligence activities are a last resort on the scale of epistemic practices. Some of the more sensitive and secretive types of intelligence collection are risky, expensive, and time-consuming. As a general rule, any effective national security information management system seeking to fulfill the knowledge requirements of its decision-makers should look to its low-cost, low-risk, and least harmful options first before turning to intelligence. Why risk exposure and loss of a valuable HUMINT asset when the same information might be freely given via diplomatic channels? So, if we are referring to epistemic practices, then I believe we can talk meaningfully about a last resort (not just logical resort) as a JIT principle.

Intelligence Institutions and Democratic Norms

A second key theme is the tension between the institutionalization of intelligence and liberal-democratic norms and values. The uneasy tension between secrecy and transparency is a problem for democracies broadly speaking. According to Zegart, for instance, American intelligence history demonstrates the difficulty of finding the right balance between the need for a government strong enough to provide security but restrained enough to protect individual rights (p. 49). When President Truman signed the law creating the CIA in 1947, he feared creating an American Gestapo and insisted the new intelligence agency have no domestic intelligence-gathering or law enforcement capabilities (pp. 49–50). There are similar concerns in Australia. For example, Australia's foreign intelligence collection agencies are prohibited from collecting intelligence on Australian citizens. According to participants in Hammond-Errey's study, this is one of the critical distinctions designed to protect citizens from "secret police" and domestic abuses of human rights. As outlined in the 2020 Richardson Review:[10] "there should be a clear separation between those agencies responsible for the collection of security intelligence, and those responsible for policing and the enforcement of the law, to avoid creating the perception—or the reality—of a 'secret police'" (p. 124). In short, when national security institutions generally, and intelligence institutions in particular, exercise more and more power over their jurisdictional inhabitants,

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

the concern is that this is the road to authoritarianism. Henschke and colleagues argue that this is why liberal democracies must seek to monitor and constrain their intelligence institutions (p. 5).

Henschke and his coauthors point out that liberal democracies face a basic tension when it comes to intelligence: many intelligence actions, and even the existence of intelligence institutions, can run counter to basic human rights and may threaten the trust in, and authority of, other democratic institutions (p. 3). In other words, intelligence actions and institutions run counter to liberal-democratic values and potentially undermine public trust in government. This is why they argue that "a comprehensive theory of intelligence practices and institutions is needed to ensure that liberal democracies do not become the very things that they are fighting against" (p. 3-4). Such a theory, they suggest, is normative since it is a theory of what intelligence practices and institutions morally *ought to be* (p. 4). In order for intelligence to do its job effectively, Henschke argues, it needs to exploit sensitive private information. The ethical challenge for liberal democracies, then, is how to do this in a way that is privacy respecting (p. 147).[11]

Participants in Hammond-Errey's study also discussed moral concerns about government intrusions and the right to privacy. For example, one participant stated that "the challenge is the appropriate balance between the individual's right to privacy" and the "shift in the threat environment" (p. 116). This participant recognized that the community expectation within a liberal democracy is that "data relating to them, within government and outside government, is only accessed and utilised for proper legislated purposes" (p. 116).[12] A key point in Hammond-Errey's study is her observation that the intelligence practitioners interviewed believe that the basis of moral legitimacy for their activities is the way they are perceived by their own citizens. This brings us back to the central role of trust (as discussed above). Many participants in Hammond-Errey's study raised their organizational values in the context of ethics. For instance, one participant mentioned the values of the Australian Signals Directorate (ASD) and commented: "Those values were not derived and imposed on the staff. They were derived from talking to the people inside the organization. It was about purpose. What do we do? We make a difference, we strive for excellence because you should strive for excellence … we operate in the slim area between the difficult and the impossible, because that does actually describe what ASD does. We obey the law because we have this enormous capability" (p. 140).

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

The Purpose of Intelligence

A third key theme is the consideration of the ultimate purpose or ends of intelligence. According to Seumas Miller, writing in *The Ethics of National Security Intelligence Institutions* (chapter 2), the acquisition of knowledge and aiming at truth is an end in itself for intelligence officers. An otherwise skilled operative who does not aim at acquiring knowledge or truth, he suggests, would not be a good intelligence officer (p. 39). Miller argues that intelligence officers who are not committed to this end are more likely to neglect the practice of truth seeking and instead focus on personal, political, or other nonepistemic gains (p. 40). While this is correct, there is a tension between the idea of intelligence as "truth seeking" and its inherent competitiveness in the national security arena, which brings into play significant amounts of deception and subterfuge, both for obtaining intelligence about an adversary and in protecting one's own secrets (that is, counterintelligence).

Furthermore, it is not merely the truth seeking that is important for intelligence; the truth telling also matters. Intelligence seeks an accurate understanding of the world not for its own sake, but for the benefit of specific decision-makers. A recurring theme throughout Hammond-Errey's study was the belief that intelligence activity seeks knowledge that benefits the decision-making of customers. For instance, one participant stated that "purpose is the most important thing … You actually have to understand what is the purpose you are doing it for? Who is the customer that is going to use that information?" (p. 86). Henschke and colleagues describe intelligence as "part of an epistemic activity, intended to change and ideally improve the understanding of the world such that decision-makers make better decisions" (p. 12). Similarly, Zegart argues that a core part of the intelligence mission is speaking truth to power. She cites her interview with former director of national intelligence Dan Coats, who said, "We strive to know the truth and we have an obligation to speak the truth. Anything short of that is a disservice to policymakers and to our country" (p. 86).[13] In short, intelligence should be understood as a knowledge-focused activity that plays a key role in national decision-making.

Another source of tension for intelligence institutions is the overlap of their work with that of other national security institutions, such as the military. Zegart makes the point that the Pentagon and CIA, for instance, were set up separately for good reason. The U.S. military's primary mission is fighting, and its officers are trained

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

in the effective use of armed force. In contrast, the CIA's primary mission is understanding, and its officers are trained in the management of sensitive information—"how to get it, analyze it, hide it from the wrong people, and share it with the right ones" (p. 193). Of course, the practices of the CIA throughout its history have hardly been so straightforward, with involvement in all kinds of covert actions and forms of political interference that have little to do with seeking understanding. This includes the use of propaganda, coups, assassinations, drone strikes, and so on and so forth. But the point to make here is that these types of activities are controversial and should not be considered within the remit of intelligence properly understood. Mary Ellen O'Connell, for instance, argued that the fact that some drone strikes were performed by the CIA (or CIA contractors) in Pakistan between 2004 to 2009 accounted for the high unintended death rate. She attributed this to the fact that CIA operatives were not trained in the law of armed conflict and were not bound by the Uniform Code of Military Justice to respect the laws and customs of armed conflict.[14] In short, the CIA is a hybrid organization and perhaps not a good example of what an intelligence institution should be.

A further area of tension is the relationship that intelligence institutions have with policymakers. Intelligence is an epistemic enterprise: it seeks to uncover secrets in order to describe the world as it is or is likely to be. In contrast, politics and policymaking is concerned with power, government, and making an impact on the world. Henschke argues, correctly, that the reason we should separate intelligence and policymaking is because we want the intelligence produced to be trustworthy (p. 181). If political actors unduly influence the outcomes of intelligence assessments (that is, intelligence becomes politicized), then intelligence becomes unreliable as an accurate guide for understanding topics of interest to decision-makers. Over time, the politicization of intelligence degrades trust in the intelligence agencies themselves. This, argues Henschke, ultimately leads to a significantly reduced capacity for intelligence actors to reliably inform political actors' decision-making (p. 178).

Secrecy, Oversight, and Trust

Finally, the fourth key theme across the three books is the notion that intelligence institutions should seek to maintain the trust of the public despite their activities being shrouded in secrecy. One of the hallmarks that distinguishes authoritarian states from liberal democracies, argues Henschke, is the lack of control of, oversight

over, and public support for intelligence agencies (p. 171). He argues that insofar as we want and need the truth to be authoritative, rather than supportive of a particular political actor or ideology, then we need to both protect and listen to our epistemic institutions. If intelligence merely reinforces the decisions of political actors in a post hoc fashion, then that political system loses its connection with reality and is on the slide into authoritarianism (p. 174).

Participants in Hammond-Errey's study held the view that citizens' trust in national security agencies is critical to their ability to operate effectively. For instance, one participant said: "Public accountability and trust are the biggest challenges [of big data for national security] … We make a really big thing of the fact that our success relies on the public's trust and anything that erodes that is generally considered a bad thing" (p. 158). What emerged strongly from Hammond-Errey's study was a sense that trust is a significant issue in the role of intelligence work; but that participants from Australia's NIC understood trust differently, depending on the function and type of community interaction of their agency (p. 155). For instance, agencies with a direct domestic security responsibility —the Australian Federal Police and Australian Security Intelligence Organisation —were the most vocal about the requirement for legitimacy and building trust with the Australian people and Australian businesses. They believed that, for their agency, maintaining trust is primarily connected to actively preventing harm (p. 165). In other words, the focus is on delivering a public good, such as public safety (p. 156). In contrast, other members of the NIC understood trust in terms of a social contract. For example, one interviewee said: "There is a social contract with government and the people that the government will keep us safe. It is why we have police officers and the military. They are there to keep us safe. The intelligence agencies are there to provide information to government to help them make clever decisions. That's a broad, rough characterisation but that's really what it is. There are security agencies for where law enforcement isn't sufficient. There is a social contract there" (p. 159).

Zegart makes the point that intelligence agencies cannot succeed without trust, and trust requires effective oversight and an understanding of the reality of intelligence work.[15] She claims that people working in intelligence believe that effective oversight is essential for building and maintaining public trust in intelligence institutions. For instance, she quotes former CIA deputy director Michael Morell, who said, "Oversight of intelligence I think is particularly important because the community is made up of a group of organizations that are secret

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

organizations operating in a democracy, and there has to be a process to assure the American people that they are operating the way they should" (p. 199).[16] Zegart argues that congressional oversight ought to be nonpartisan and operate at a high level. It should ensure that intelligence agencies get the resources they need, set agencies' strategic priorities, maintain accountability, and check compliance with the law. The purpose of such oversight, suggests Zegart, is to maintain public confidence in intelligence institutions that "must, by necessity, hide much of what they do" (p. 199).

Conclusion

All three books address the complex and constantly evolving ethical dilemmas faced by intelligence institutions operating in liberal democracies. Their methodological approaches differ significantly, but this diversity is ultimately complementary. Henschke and colleagues are unabashedly focused on developing ethical theory; in particular, lower-level normative or value theories that operate within specific institutional, occupational, and technological settings. The novel premise of *The Ethics of National Security Intelligence Institutions* is that we need to look at intelligence institutions, not simply the acts and practices of intelligence, for a thoroughgoing understanding of intelligence ethics. In contrast, the value of Zegart's and Hammond-Errey's research, in their respective books, is the access each of them provides to the thoughts and opinions of the intelligence practitioners working in these secretive institutions. If you ask intelligence officers what misperceptions bother them most, writes Zegart, odds are they will mention ethics. "People think we're lawbreakers, we're human rights violators," says former CIA counterintelligence chief James Olson (p. 95).[17] It is true that intelligence practitioners have been lawbreakers and human rights violators, but that is neither all they are nor all that they do. The historical secrecy of intelligence institutions might give the impression that intelligence is an ethics-free zone, but the books reviewed here demonstrate that this is certainly not the case.

Notes

[1] Amy Zegart makes the point that up until the (mid)twentieth century, intelligence was considered a strictly wartime endeavor, not a peacetime capability to help policymakers gain advantage in international affairs. It was only after World War II that permanent, robust peacetime intelligence capabilities took hold (p. 46). She points out that the U.S. intelligence community is now vast, comprising eighteen federal agencies and roughly one hundred thousand people. In 2021, the total intelligence budget was an estimated $85 billion (p. 82). See Amy B. Zegart, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* (Princeton, N.J.: Princeton University Press, 2023).

[2] For some of these recent debates, see: Cécile Fabre, *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence* (Oxford: Oxford University Press, 2022); Seumas Miller, Mitt Regan, and Patrick F. Walsh, *National Security Intelligence and Ethics* (Abingdon, U.K.: Routledge, 2021); Jai Galliott and Warren Reed, *Ethics and the Future of Spying: Technology, National Security and Intelligence Collection* (Abingdon, U.K.: Routledge, 2016); and Ross W. Bellaby, *Ethics and Intelligence Collection: A New Framework* (London: Routledge, 2014).

[3] They explicitly distinguish their lower-order, context-dependent approach to theory, however, from much of the philosophical work undertaken in universities in the English-speaking world over the last century, which, they suggest, has been concerned with higher-order abstract theory.

[4] For an argument supporting the moral exceptionalism of the JWT, see Shannon Brandt Ford, "Moral Exceptionalism and the Just War Tradition: Walzer's Instrumentalist Approach and an Institutionalist Response to McMahan's 'Nazi Military' Problem," *Journal of Military Ethics* 21, no. 3-4 (2022), pp. 220– 27.

[5] See the following edited collections for early work on intelligence ethics: Jan Goldman, *Ethics of Spying: A Reader for the Intelligence Professional*, vol. 1 (Lanham, Md.: Scarecrow, 2006); and Jan Goldman, *Ethics of Spying: A Reader for the Intelligence Professional*, vol. 2 (Lanham, Md.: Scarecrow, 2010).

[6] Fabre, *Spying through a Glass Darkly.*

[7] See, for example, Megan Braun and Daniel R. Brunstetter, "Rethinking the Criterion for Assessing CIA-Targeted Killings: Drones, Proportionality and *Jus Ad Vim*," *Journal of Military Ethics* 12, no. 4 (2013), pp. 304–24; and S. Brandt Ford, "*Jus Ad Vim* and the Just Use of Lethal Force-Short-of-War," in Fritz Allhoff, Nicholas G. Evans, and Adam Henschke, eds., *Routledge Handbook of Ethics and War: Just War Theory in the Twenty-First Century* (New York: Routledge, 2013), pp. 63–75.

[8] Michael Quinlan, "Just Intelligence: Prolegomena to an Ethical Theory," *Intelligence and National Security* 22, no. 1 (February 2007), pp. 1–13.

[9] An interesting follow-up study would be to examine historical cases where the ROT principle applies.

[10] The "Richardson Review" examined the effectiveness of the legislative framework governing the Australian national intelligence community and published its findings in 2020. See *Comprehensive Review of the Legal Framework of the National Intelligence Community* (Commonwealth of Australia, 2020) www.ag.gov.au/national-security/publications/report-comprehensive-review-legal-framework-national-intelligence-community. It was led by former secretary for the Australian Department of Defense Dennis Richardson, companion of the order of Australia.

[11] Henschke says that rather than understanding privacy merely as the relationship between two people (interpersonal privacy), when considering intelligence, we need to see that government and citizens may be the key actors shaping our analysis. Similarly, with the rise of information technologies, the key actors framing our analysis will be companies and customers. At this layer of analysis (institutional privacy), the moral authority and legitimacy of the institution shape the ethical analysis of privacy. Furthermore, we have a third layer of analysis in which the key actors are states (international privacy) (p. 159).

[12] There's also the question of privacy for nonintelligence institutions (which I cannot address here), given the access some companies may be forced to provide; for instance, via encryption debates like those concerning Telegram in France and Apple in the United States.

[13] Interview by Zegart, September 25, 2020.

[14] Mary Ellen O'Connell, "Unlawful Killing with Combat Drones: A Case Study of Pakistan, 2004–2009," in Simon Bronitt, Miriam Gani, and Saskia Hufnagel, eds., *Shooting to Kill: Socio-Legal Perspectives on the Use of Lethal Force* (Oxford: Hart, 2012), pp. 263–92, at p. 270.

[15] Zegart believes that most Americans, including members of Congress, cabinet officials, and judges making policies affecting national security, do not know much about the actual world of intelligence. Fictional portrayals of intelligence—as in movies, TV, books, and so forth—too often substitute for fact, she concludes, creating fertile ground for conspiracy theories to grow and influencing the formulation of real intelligence policy.

[16] Michael Morell, quoted in Zegart, *Spies, Lies, and Algorithms*, p. 199; Michael Morell, Intelligence Matters, Special Edition Episode on Congressional Oversight, with Sen. Saxby Chambliss, Sen. Bill Nelson, Rep. Jane Harman, and Rep. Mike Rogers, March 29, 2019.

[17] Interview by Zegart, October 13, 2020.

Abstract: The secrecy of intelligence institutions might give the impression that intelligence is an ethics-free zone, but this is not the case. In *The Ethics of National Security Intelligence Institutions*, Adam Henschke, Seumas Miller, Andrew Alexandra, Patrick Walsh, and Roger Bradbury examine the ways that liberal democracies have come to rely on intelligence institutions for effective decision-

https://doi.org/10.1017/S089267942510004X Published online by Cambridge University Press

making and look at the best ways to limit these institutions' power and constrain the abuses they have the potential to cause. In contrast, the value of Amy Zegart's and Miah Hammond-Errey's research, in their respective books, *Spies, Lies, and Algorithms: The History and Future of American Intelligence* and *Big Data, Emerging Technologies and Intelligence: National Security Disrupted*, is the access each of them provides to the thoughts and opinions of the intelligence practitioners working in these secretive institutions. What emerges is a consensus that the fundamental moral purpose of intelligence institutions should be truth telling. In other words, intelligence should be a rigorous epistemic activity that seeks to improve decision-makers' understanding of a rapidly changing world. Moreover, a key ethical challenge for intelligence practitioners in liberal democracies is how to do their jobs effectively in a way that does not undermine public trust. Measures recommended include better oversight and accountability mechanisms, adoption of a 'risk of transparency' principle, and greater understanding of and respect for privacy rights.

Keywords: intelligence, applied ethics, international norms, secrecy, institutions, national security, just war theory, big data, trust, privacy rights