Reply to Critics

*Cécile Fabre**

In my recent book *Spying through a Glass Darkly*, I provide a normative defense of espionage and counterintelligence activities in the service of foreign policy goals. Such a defense must show at least two things. First, it must show which foreign policy goals, if any, provide a justification for such activities. Second, it must provide an account of the means that intelligence agencies are morally permitted, indeed morally obliged, to use during those activities. On the first count, I argue that espionage and counterintelligence are morally justified only as a means to protect individuals' fundamental moral rights to the freedoms and resources they need to lead a flourishing life. I also claim that the point applies to economic espionage. On the second count, I discuss the ethics of using human sources such as informants and of a range of technologies such as old-fashioned listening devices and cameras and, more problematically, cyber intelligence.

It is an honor to have the arguments from my book serve as the centerpiece of the symposium organized by Juan Espindola for this issue of *Ethics & International Affairs*, and I am grateful to have the opportunity to engage with my critics' insights. The five contributions to the symposium discuss some aspects of both justificatory tasks. I first tackle Ross Bellaby's probing critique of my defense of economic espionage. I then turn to Ron Dudai's, Alex Leveringhaus's, Juan Espindola's, and Rhiannon Neilsen's essays, which consider the ethics of the means of espionage and counterintelligence. Throughout, I

Cécile Fabre, University of Oxford, Oxford, England (cecile.fabre@all-souls.ox.ac.uk)

*I am deeply grateful to Juan Espindola for organizing this symposium, to the editors of *Ethics & International Affairs* for publishing it, and, in addition to Espindola himself, Ross Bellaby, Ron Dudai, Alex Leveringhaus, and Rhiannon Neilsen for their constructive and illuminating discussions of the book.

Ethics & International Affairs, 37, no. 2 (2023), pp. 193–205.

doi:10.1017/S0892679423000175

imagine that a political actor, Green, is the target of wrongful threats to the vital interests of its members (or of a third party) at the hands of another political actor, Blue. Green and Blue need not be nation-states: they can be guerrilla groups or organized national liberation movements.

Economic Espionage

Many states—in particular China, but also others such as France—routinely instruct their intelligence agencies to carry out economic espionage on behalf of their private companies so as to help the latter secure a competitive advantage over rivals, to promote the welfare of their populations, or both. Yet, the scant philosophical literature on espionage is silent on this age-old practice. It is fair to say, however, that, by and large, in public discourse economic espionage has received bad press: it is often regarded as tawdry, ignoble, and beyond the pale of what states are morally allowed, let alone morally obliged, to do. I am particularly pleased therefore that Ross Bellaby's piece, which is a response to chapter 4 of my book, focuses on it.

In *Spying through a Glass Darkly*, I define "economic espionage" as "the practice of acquiring secrets from private economic actors"[1] and defend it as follows: "Suppose that Green and Blue are at war, both kinetic and cyber. Corporation Weapons Inc. supplies Blue with military weapons and technology, while corporation InfoSys Inc. supplies its forces with IT resources. Suppose that Blue is the unjust aggressor. Green's firms are struggling to compete with Blue's, as a result of which Green is losing the war. Its leaders are morally justified in seeking to uncover relevant economic information about Weapons Inc. and InfoSys Inc., in the hope of undermining both firms by engaging in economic warfare and taking advantage of those firms' research and development activities."[2] Ex hypothesi, Blue is threatening the fundamental moral rights of Green or some third party, such as Green's ally. Economic espionage is justified as a means to protect those rights.

In his penetrating critique, Bellaby argues that economic espionage is not as straightforwardly permissible as this seemingly uncontroversial example suggests. For a start, much of economic espionage is driven not by the need to protect citizens from undue threats to their fundamental moral rights, but by states wanting to give a competitive advantage to their firms. The harms accruing to the targets of those activities are disproportionate to the benefits the activities bring about.

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

I agree. In fact, I explicitly state in the book that economic espionage for ends other than the protection of fundamental rights is not morally permissible.[3] Admittedly, the line between critical and noncritical cases is not as sharp as I may be suggesting in the book. Whether economic espionage is morally justified in gray-area cases partly depends on the risks to which Green would expose those individuals it is seeking to protect by refusing to spy on, for instance, InfoSys Inc., relative to the risks it would inflict on firms that are only very loosely related to Blue's war efforts if it did spy. However, the claim that Green ought to exercise extreme caution (which is where, I think, Bellaby wants to go) does not undermine the thesis that in clear cases, it may spy.

That being said, even in cases in which the activities of a private firm undermine or risk undermining Green's critical infrastructure, thereby posing a threat to its citizens' fundamental moral rights, Bellaby rejects those practices. Firms operate in a competitive environment. When Green spies on a Blue firm to protect its infrastructure, it all too often deliberately undermines *Blue's* infrastructure and, in so doing, deliberately harms Blue's innocent citizens who are dependent on it—in violation of the principle of discrimination between (loosely put) the innocent and the guilty.

I see the force of Bellaby's point. His example—in which Green drives Blue out of being able to buy critically necessary oil from a supplier, thanks to having discovered crucially important economic intelligence—illustrates it well. When economic espionage is a means to gain a competitive advantage over a rival, given the zero-sum-game nature of the competition, it is hard to see how it can avoid breaching the requirement to avoid deliberately harming the innocent. Note, however, that economic espionage need not always take that form. We can imagine a variant of my own example in which Green's espionage activities against InfoSys Inc. and Weapons Inc. enable its leaders to fight their war against Blue more effectively (for example, by developing new weapons technologies), but without attacking Blue's infrastructure.

I suspect that Bellaby would reject this response and insist that even in such cases the harms accruing from economic espionage are much greater than I allow in the book and run afoul of the requirement of proportionality. Whether he is right requires a more careful empirical investigation than I can provide here, indeed than has been provided in the literature, at least to my knowledge. But *if* he is right, then I would have to agree with him and reject the practice, on those grounds. Note, though, that by the same token, one would have to reject

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

any kind of espionage activity found to be disproportionately harmful to the innocent—including espionage of the more standard military kind. One of my core points in the book would survive this inquiry—namely, that the nature of the information about Blue that Green seeks to acquire, whether it be political, military, or economic, does not make a difference to the *in-principle* morality of espionage.

Informants, Counterinsurgency, Counterterrorism, and New Wars

My defense of espionage and counterintelligence is not meant to be state centered. Indeed, as I note early on, nonstate actors can and do conduct such operations in the pursuit of goals that, if they were states, would be aptly called "foreign policy goals." As for states, they conduct such operations not merely against one another but also against nonstate actors: when MI6 (Britain's secret intelligence service) uses informants to gather information on a cell of DAESH, the Arabic acronym for the transnational militant Islamist group also known as ISIS (or ISIL), it is unquestionably spying on the latter.[4] Yet, Ron Dudai argues in his essay that for all that I aspire to unmoor espionage from the statist, Cold War–inspired framework that we—in the Anglophone world at least—have inherited from John le Carré's novels,[5] much of my normative analysis highly depends on it. The problem, according to Dudai, is that the statist approach considerably restricts its scope.

Dudai accepts that espionage is morally justified as a means to protect fundamental moral rights, subject to the requirements of necessity, proportionality, and effectiveness; he also accepts that the recruitment of inside informants to that end is morally justified, indeed mandatory, even though those assets will be treated and punished as traitors if they are found out. Nevertheless, outside state-on-state espionage, in the "messier reality of counterinsurgency, counterterrorism, and 'new wars,'"[6] the use of informants is so widespread as to be a form of mass recruitment, and occasions a range of individual and societal harms. In asymmetrical conflicts between state and nonstate actors, state agencies aim not so much to protect rights as to control their own population. Informants are recruited not just by intelligence services but also by armed forces and law enforcement agencies, all of which have a much broader range of coercive tools at their disposal to do so than what intelligence agencies have in traditional war contexts. Moreover, informants sow distrust among the community in which they operate (which is often

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

the point); they and their relatives are vulnerable to severe reprisals at the hands of armed rebel groups; and communities targeted by mass recruitment are less likely to trust state authorities and, as a result, to volunteer information that would help save lives. Once those harms are properly accounted for, they render those operations disproportionately harmful and, by my own lights, should be impermissible.

Dudai brings an illuminating sociological dimension to the ethics of espionage. I entirely take his point that a justification for the recruitment of informants must be sensitive to the long-term and societal harms that it causes. Accordingly, I have no difficulty conceding that to the extent that mass recruitment is harmful in the ways he suggests, it simply cannot be justified. I also accept Dudai's call for a proper public debate about the use of informants in general, and his proposal in favor of much more targeted and tightly regulated recruitment. As he also rightly notes, devising the right kind of regulatory regime is beyond the scope of his, and my, inquiry.[7] That said, let me make three points. First, institutional design of that kind requires a delicate balancing act between the demands of secrecy, necessary in part to protect existing human sources, and the demands of transparency, necessary in part to render intelligence agencies properly accountable. It is hard to see how we can adjudicate between those competing demands by appealing to general principles in abstraction from the specific context of the domestic politics and geopolitical stakes in which those institutions operate.

Second, institutional design is not enough. Forbidding case officers to use sexual blackmail as a recruitment strategy is easy. Working out whether a potential informer is properly aware of the risks he is incurring and of the toll his work might take on his family life is not. Intelligence officers will always need scope to exercise their moral judgment about individual cases. To be a good recruiter in the messy reality of counterterrorism and counterinsurgency requires a particular kind of practical wisdom that is not easy to cultivate. I take it that Dudai would agree with both points.

Finally, we must also reckon with the moral costs of eschewing mass recruitment: it is perfectly possible that, notwithstanding the greater benefits of slimmed-down intelligence institutions over the long term, our inability to gather certain kinds of information would in the short term occasion considerable harms, indeed leading to a loss of lives. That may well be a price worth paying; but at least let us be aware of it.

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

The Technology of Espionage

In their contributions, Leveringhaus, Espindola, and Neilsen focus on the ethics of espionage technology and cyber intelligence. Leveringhaus argues that I overemphasize similarities and downplay differences between the use of technologies relative to the use of human sources. Espindola and Neilsen consider two emerging technologies for collecting and handling data, both of which, they claim, can play a useful role in preventing the commission of crimes against humanity and war crimes: facial recognition technology, on the one hand, and cyber manipulation, on the other.

Problematizing Technology

Suppose that Green's intelligence agencies have reasons to believe that Blue—a quasi-state organization intent on territorial conquest—is planning to attack Green via a combination of conventional and terroristic means. To thwart the attack, Green needs to procure more information than it currently has on the intentions of Blue's leaders and on its operational resources. Suppose further that it can choose between placing a human source in the entourage of Blue's main leader or planting spying devices in his house. Other things equal, I argue, Green is under a moral duty to opt for the latter: infiltrating an asset is far riskier, not least to that person, than eavesdropping from afar.[8]

Leveringhaus accepts, indeed constructively strengthens, my argument for such cases. However, he also points out that technology rarely acts as a like-for-like replacement for human sources; likewise, emerging technologies (such as insect-like robots) rarely act as a like-for-like replacement for new technologies (such as phone taps.) Just as we now worry that precision weaponry is not the moral panacea we may have thought it to be at first, so we should worry that espionage and counterintelligence technologies are so cost effective as to induce intelligence agencies and their political masters to misuse them. In the absence of those technologies, they might have thought twice before using more expensive and more vulnerable human sources; they might be more willing to solve global crises through collaborative mechanisms instead of resorting to economic espionage; they would be less likely to harm the innocent by harvesting information about them that in turn is fed into AI processes and forms the basis for cyber-intelligence operations; and they would be less likely to blur the line between intelligence operations and acts of war.

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

Leveringhaus's essay is a welcome intervention not merely in the ethics of espionage but, more generally, in the (as-yet-underdeveloped) ethics of weapons development. Much of what he says applies to technological developments of the past, some of which did once raise similar concerns: at the risk of rehearsing a tired trope, in the wake of Germany's destructive use of U-boats during the First World War, voices could be heard in Britain calling for a ban on submarine warfare. This is not to downplay the force of Leveringhaus's criticism. Rather, it is to bring into relief both a methodological issue to which I only briefly allude in the book and a deeper normative question that I do not properly tackle. The methodological issue is this: If, as Leveringhaus says and as I acknowledge in the book,[9] Green must judge on a case-by-case basis whether to use a given emerging technology, then it seems that one cannot speak of the ethics of technology in general. This, perhaps, casts doubt on the robustness of this emerging field of applied ethics.

The (more interesting) normative question is this: At the end of his essay, Leveringhaus wonders whether "states should sometimes forgo the development of certain spy technologies if their long-term effects would be extraordinarily detrimental."[10] Yet, in the case at hand, we do not know what the mid- and long-term consequences of an unregulated developing technology are; nor do we know whether regulation will be effective. What, then, are we morally permitted to do under conditions of uncertainty? On the one hand, we might be tempted to appeal to some version of "the precautionary principle." Roughly put, if a given course of action is more likely than not to cause serious harm and if we do not really know what exactly the causal connection is between the two, or what exactly is the probability that the harm will occur, or whether we will be able to take mitigating steps, then we ought to desist altogether, or at the very least postpone until we have more information. On the other hand, we—or, rather, political leaders acting on our behalf and at our behest—must know that even if *we* desist, other actors, and particularly our enemies, will not. In the face of noncompliance, it seems impermissibly imprudent to adopt the precautionary principle. The solution—imperfect though it is—may well lie in international cooperation of the kind that saw the adoption of international conventions against certain kinds of weapons.

Facial Recognition and Mass Surveillance

In the weeks leading up to Russia's invasion of Ukraine and since then, Ukraine's intelligence agencies have harvested facial images of dozens of thousands of

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

Russian young men from social media accounts, and have triangulated those images with photos of Russian soldiers on the front line, or of men suspected of sabotage or of espionage activities in occupied areas. Thanks to facial recognition technology (FRT), notably through the services of Clearview AI, they have then been able to identify some of those men by name. Ukraine has claimed that this is serving three purposes: identifying and arresting suspected spies and saboteurs operating under civilian cover; identifying Russian soldiers who are suspected of having committed war crimes, with a view to prosecuting them; and identifying dead soldiers to notify their relatives back in Russia. As Espindola suggests, Ukraine can thus hope to justify FRT as a means to protect its civilians; to bring war criminals to justice; and to fulfill its duty of care to the families of those combatants, notwithstanding the fact that they are Ukraine's enemies.

That being said, the use of FRT raises three concerns: it invades the privacy of those soldiers; it is a slippery slope leading to civilians' increasing tolerance of a technology that, though justified by those wartime ends, nevertheless would constitute an unjustified breach of privacy once the war is over; and, when used to identify fallen soldiers, it causes severe distress to their families, is driven by the hope of mobilizing them into resisting the invasion, and amounts to a form of psychological warfare. On Espindola's view, the privacy objection is not particularly strong, as Russian soldiers and spies have forfeited their right not to be spied upon. However, the other two concerns must be taken seriously. In particular, "whether the wartime benefits of FRT outweigh its postbellum risks is a matter to be decided contextually."[11]

This is a fascinating issue. Espindola is right that my arguments in favor of data collection, in the book's final chapter, seem to lend themselves to endorsing FRT. He is right, too, to draw attention to the importance of prosecuting war criminals and of belligerents' duty of care to enemy civilians. I do not address either of those issues in the book. But without going as far as resorting to FRT, one can imagine a case in which Green's agencies resort to old-fashioned espionage while the war is ongoing to collect information that, its leaders know, will be useful should it decide to initiate proceedings against war criminals. Likewise, Green might use human sources to photograph the name tags of dead enemy soldiers and pass on the information to families.

However, I am more explicitly critical—less on the fence, if you will—than Espindola when it comes to facial recognition, particularly as it has been used

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

by Ukraine, for two reasons. First, as he notes, the technology is developed and sold by profit-driven private corporations, which has given cause for concerns, notably about Clearview AI. For example, in May 2022, the Information Commissioner's Office in the U.K. imposed a £7.5-million fine on the company. Clearview AI had not informed the British social media users whose images it had harvested for its online database that these images were being sold to law enforcement agencies around the world. Clearview AI continues to operate in the United States notwithstanding several lawsuits. Similar concerns have been raised about Chinese companies exporting their FRT platforms with little or no oversight.[12] It seems to me that the peacetime, or postbellum, harms accruing from FRT *do* outweigh its wartime benefits.

Second, even if the jury is out on this point, I give greater weight to Espindola's worry about wartime use than he seems to do. Posting images of identified dead soldiers online so that their families may learn of their fate and take steps to collect their bodies does in fact morph into a particularly intrusive form of psychological warfare. That alone disqualifies this particular use. To be clear, my claim is not that psychological warfare is in itself morally impermissible: this would rule out many forms of wartime propaganda and might be a step too far. My point, rather, is that there are other, less harmful ways to relay such dreadful news to families—such as the international tracing service of the Red Cross—that do not involve public dissemination.

By implication, FRT without public dissemination is morally justified as a way to exercise a duty of care to the dead and the bereaved, so long as the way in which it operates (such as the nonconsensual harvesting of identifying images) is not morally wrong. It might also be that concerns about its abuses in peacetime can properly be dealt with through regulation and enforcement thereof. Still, I conclude that, absent further arguments to the contrary, intelligence agencies and their military and civilian leaders should not use it as a tool of war.

Cyber Manipulation

In the book, I argue that intelligence agencies are morally justified, indeed sometimes morally obliged, to conduct two kinds of operations (inter alia): (a) deception operations such as those carried out by the Allies against Nazi Germany during World War II; (b) hacking into the enemy's cyberinfrastructures as means to, for example, break into and damage its cyberdefense, or to steal vital communications between its top commanders.

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

Neilsen's thought-provoking contribution combines those two claims into a defense of what she calls "cyber manipulation operations" (CMOs), as a means to stop atrocities such as crimes against humanity, genocide, and other war crimes. Suppose that Green has reliable information that Blue is preparing a genocidal campaign against a long-oppressed minority within Blue. Green, together with other members of the international community, has attempted to persuade Blue's leadership not to go ahead—it seems to no avail. Green's intelligence agencies have the capacity to hack into Blue's cyber-systems and to (for example) make it appear as if Blue's generals are ordering troops to delay deployment or to relocate away from areas densely populated with members of the targeted minority; to cancel orders for ammunitions and supplies needed to build extermination facilities; to prevent addressees of emails from receiving headquarters' communication without anyone being the wiser, and so on. Unlike "traditional" deception operations, such as turning over enemy intelligence agents and feeding them false information that they then relay to the enemy, CMOs dispense with the need to rely on human sources. Unlike cyber sabotage or the cyber operations that I describe in the book, CMOs do not seek to steal the enemy's information or to damage its cyber infrastructure: rather, they intervene on the information that is already present in the enemy's systems or create information that must be seen to originate therefrom; and it is crucial to their success that those systems continue to work.

On Neilsen's account, CMOs are morally justified on the ground that they help prevent atrocities, that they are less costly than, for instance, full-scale military interventions or even economic sanctions, and that by confusing Blue, they help Green buy time to take steps toward those more forceful responses should Blue persist. They are also more efficient than outright cyber-sabotage, for they are harder to detect and less likely to alert Blue that its cyber-defenses have been breached. In fact, under those circumstances, they might even be morally mandatory.

I am broadly sympathetic to Neilsen's view. I agree that my arguments in favor of deception and cyber espionage together open the door to morally justified operations of cyber manipulation along the lines that she has suggested, at least as a means to stop atrocities. I also agree that in any given case, Green's leaders must pay close attention to the consequences, whether intended or not, of such an operation. Particularly worrisome is the risk that if Blue discovered that Green has cyber manipulated the orders issued by its commanders to troops,

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

the latter would have no reason to trust in the veracity of such orders—including *genuine* orders to lay down arms and respect a ceasefire. However, I am skeptical of Neilsen's response. She suggests that

> the head of state ought to be exempt from impersonation via CMOs. It is paramount to preserve his legitimate authority, precisely because he . . . is the only person who can order an end to the atrocities. Conversely, middle- and lower-ranked military or government leaders may be justly impersonated . . . because their influence is not as far-reaching.[13]

This presupposes that the head of state *has* legitimate authority in general, and the authority to end the war in particular, even if he did order his troops to commit grievously wrongful acts at the start of the campaign. As a matter of law, that is correct. As a matter of morality, however, it is not so clear. It may well be that, as a matter of fact, President Putin alone would be able to halt the war in Ukraine and its concomitant atrocities, in the sense that Russian armed forces would lay down their arms only on his say-so; but it does not imply that his say-so is morally transformative—that it confers on those armed forces a duty, which they did not have before, to lay down their arms; for that, in fact, is what they ought to do, morally speaking, here and now, irrespective of President Putin's say-so.[14]

But let us assume that there is a sense in which Blue's president can, either de facto or de jure, order an end to the war. Even so, I am not sure that we can so easily draw a line between the head of state, on the one hand, and middle- and low-ranked military and civilian officials, on the other. (I wonder, incidentally, on which side of the line highly ranked officials fall.) Suppose that Blue's president declares that he is willing to enter peace negotiations with Green, and that troops must observe a ceasefire. His order must be relayed and given effect by middle- and low-ranked officers to the troops. If Blue's rank-and-file troops and citizens learn that Green's agents have cyber impersonated those officials during the conflict, it is hard to see why they would believe in the veracity of the latter's instructions. Granted, they are likely to have access to other means of information: they might see on Twitter, for example, that the president has declared an end to the war. But, again, if they know that Green has carried out a CMO against some Blue officials, why would they believe that their head of state has not been impersonated as well? Or suppose that the head of state genuinely does want and call for a ceasefire but that his main rivals for the leadership are hardliners. It would be in the latter's interest to claim, falsely, that Green has cyber impersonated him.

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

To be clear, I agree with Neilsen that this kind of CMO risks jeopardizing prospects for peace. Indeed, it is a strength of her account that it is sensitive to the imperative of ending wars. It seems to me, however, that the line ought to be drawn not between the head of state and middle-/low-ranked officials, but between impersonating officials and falsifying their orders, on the one hand and, on the other, falsifying information in respect to logistics (such as requests for munitions or blueprints for weapons), the location of victims, or mission outcomes. This is because in most cases, prospects for an all-things-considered just peace rest with orderly peace negotiations. Those negotiations require for their success not just that belligerents have some minimum degree of trust in one another but also that their citizenries have some trust that what their leaders and officials report to them about those attempts to end the war genuinely reflects their leaders' and officials' words, not the words of impersonators.

Conclusion

Taken together, the five symposium essays bring into salience at least three issues. First, the long-term societal consequences of certain kinds of espionage, and certain means for procuring information, are more harmful than I have allowed for in the book. Second, and relatedly, stylized case studies and hypothetical examples involving individual agents only take us so far when dealing with a phenomenon as complex as espionage and counterintelligence. At the same time, these examples do bring some degree of clarity, not least in helping us ascertain what normative principles should in general guide individual actions and institutional reforms —particularly the requirement of proportionality. Third, the practice of espionage, particularly when it comes to technology, is evolving fast and in directions that seemed unthinkable until not so long ago. This is not a reason to abandon those principles altogether in favor of new radically different principles; rather, it is yet a further reason to interpret them in a context-sensitive way.

Notes

[1] Cécile Fabre, *Spying through a Glass Darkly: The Ethics of Espionage and Counter-Intelligence* (Oxford: Oxford University Press, 2022), p. 72.
[2] Ibid., p. 82.
[3] Ibid., pp. 73–74, 89.
[4] Ibid., p. 6. See "British Intelligence Explained," Secret Intelligence Explainer M16, www.sis.gov.uk/intelligence-explained.html for a fictional but plausible description of an MI6 operation along those lines.

https://doi.org/10.1017/S0892679423000175 Published online by Cambridge University Press

[5] At least his Cold War novels: as Dudai rightly notes, Le Carré's post-1990 writings are much more critical of Western agencies and the so-called War on Terror that they have helped wage at the behest of their governments and with, apparently, the support of many of their fellow citizens.

[6] Ron Dudai, "Tinker, Tailor, Soldier, *Informer*: Revisiting the Ethics of Espionage in the Context of Insurgencies and New Wars," *Ethics & International Affairs* 37, no. 2 (Summer 2023), p. 136.

[7] The *Covert Human Intelligence Sources: Revised Code of Practice* report, which the U.K. Home Office published in December 2022 and which seeks to provide guidance to public authorities such as the police, the Security Service (MI5), and the Secret Intelligence Service (MI6) makes it very clear that theoretical examples, which help frame the guidance, cannot "replicate the level of details to be found in real cases" (sec. 1.7). See Great Britain Home Office, *Covert Human Intelligence Sources: Revised Code of Practice* (London: Home Office, December 2022), assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1123687/Revised_CHIS_Code_of_Practice_December_2022_FINAL.pdf.

[8] Fabre, *Spying through a Glass Darkly*, pp. 178–181.

[9] Ibid., p. 181.

[10] Alex Leveringhaus, "Technology in Espionage and Counterintelligence: Some Cautionary Lessons from Armed Conflict," *Ethics & International Affairs* 37, no. 2 (Summer 2023), p. 161.

[11] Juan Espindola, "Facial Recognition in War Contexts: Mass Surveillance and Mass Atrocity," *Ethics & International Affairs* 37, no. 2 (Summer 2023), p. 192.

[12] See "ICO Fines Facial Recognition Database Company Clearview AI Inc More than £7.5m and Orders UK Data to Be Deleted," Information Commissioner's Office, May 23, 2022, ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/. See also Alex Hern, "TechScape: Clearview AI Was Fined £7.5m for Brazenly Harvesting Your Data—Does It Care?," *Guardian*, May 25, 2022; and Will Knight, "China Is the World's Biggest Face Recognition Dealer," *Wired*, January 24, 2023.

[13] Rhiannon Neilsen, "Cyber Intelligence and Influence: In Defense of 'Cyber-Manipulation Operations' to Parry Atrocities," *Ethics & International Affairs* 37, no. 2 (Summer 2023), p. 175.

[14] I explore this issue in greater detail in Cécile Fabre, *Cosmopolitan Peace* (Oxford: Oxford University Press, 2016), pp. 28–34.

Abstract: A normative defense of espionage and counterintelligence activities in the service of foreign policy goals must show at least two things. First, it must show which foreign policy goals, if any, provide a justification for such activities. Second, it must provide an account of the means that intelligence agencies are morally permitted, indeed morally obliged, to use during those activities. I first discuss Ross Bellaby's probing critique of my defense of economic espionage. I then turn to the other four essays, which consider the ethics of the means by which espionage and counterintelligence activities are conducted.

Keywords: espionage, counterintelligence, face recognition software, economic espionage, treason, cyberespionage, ethics of weapons development