ONE

Accountability and Intelligence

This chapter explores what is meant by accountability in the intelligence realm and considers why holding intelligence practitioners to account is seen as particularly challenging. Is there something inherent to the practice that makes accountability so difficult? Or is it more the way intelligence is framed and how secrecy is used to close off discussion and direct criticisms toward certain specific areas rather than others? To consider how intelligence and accountability interrelate, this chapter will address some basic questions, such as: what does accountability mean in this sphere? Why is it important? Who should practice it? What is it supposed to achieve? The focus of this discussion will be the secondary literature from "external" commentators. Analyzing these interpretations will provide a useful context and framework for the later chapters exploring the understandings of accountability in a national and international context, among overseers, commentators, and practitioners.

What Does Accountability Mean in an Intelligence Context?

Accountability can be defined in a number of ways. In the public policy literature, it is variously described as the "exchange of reasons for conduct,"[1] the "enforcement of standards and the fulfilment of obligations,"[2] "responsiveness,"[3] and "providing answers for your behavior."[4] Although linked, each of these indicates a different interpretation of what this term connotes—from sharing knowledge to enforcing norms, allocating responsibility or rationalizing and justifying action. A common thread across most definitions is the idea of accountability as a process whereby one actor provides an account of themselves and their behavior to another individual or group. A predefined role and set of responsibilities for the account giver are usually implied, along with parameters of appropriate behavior. The receiver is there to judge how far they have fulfilled their duties, in a way commensurate with the role and its associated norms. (The account receiver could be internal or external to the organization, depending on the circumstances.)

Accountability is therefore broadly comprised of two components: "rendering account," which is the provision of information, and "holding to account," whereby a judgment is made about the appropriateness of behavior, based on this and other information.[5] Furthermore, as noted in the introduction, the actions of the intelligence and security agencies are usually appraised according to their perceived efficiency, effectiveness, and ethics.[6] These three categories are explored in more depth later in this chapter.

In practical terms, rendering an account involves giving a narrative of what actions were taken, by whom, when, and why. In order for it to be intelligible to a third party, this narrative requires an explanation of the context to these actions, setting them within a particular time and space. A rich account could therefore entail sharing a significant amount of information about what took place and why. For this reason, accountability is problematic for intelligence agencies since secrecy and the restriction of information to as few people as possible has traditionally been central to their practice.[7] Yet accountability can take place within as well as outside an organization, and so account-giving is not precluded in the intelligence realm, provided the receiver is within the "ring of secrecy."

The accountability literature tends to draw a distinction between public accountability—between organizations and external bodies—and bureaucratic accountability, which is internal to an organization.[8] Broadly, public accountability takes legal and political forms and is about public control and democratic participation; meanwhile, internal accountability is focused on technical performance and the upholding of professional standards.[9] However, the division is not straightforward in practice since failures in performance or professional norms have legal and political consequences and public scrutiny is supposed to check for malfeasance and inefficiency.[10] Nevertheless, discussion of accountability in the intelligence realm overwhelmingly focuses on external public accountability at the expense of internal aspects.

In the intelligence field, the label "oversight" is often applied to describe forms of public accountability via legislative scrutiny bodies, inspectors general, or commissioners. The term connotes a detached, external observer providing a general level of scrutiny in a limited fashion. It is important to note that this type of public accountability is elite-focused: accountability is what happens when the heads of intelligence agencies provide a narrative of their behavior to, and answer questions from, external scrutiny bodies or informed individuals in the legislature, judiciary, or executive. Internal bureaucratic accountability, whereby officials are accountable to their line managers and so on up the chain to the head of the organization, is rarely mentioned. Nor is there much suggestion that public bodies should be able to seek accounts from lower-level officials about the workings of the intelligence agencies. Depending on the issue, the emphasis is on either the head or the minister providing an account to external interested parties.

This is a broad feature of much civil service accountability in the United Kingdom, but it is taken to the extreme in the case of the intelligence services. It is worth recalling that other forms of accountability are possible. For example, under a system of collective accountability, any member of the organization can be called to account for the actions of the group.[11] Alternatively, in a system of individual accountability, individuals at any level in the bureaucracy can be questioned about their actions and their responsibility for collective outcomes.[12] Focusing accountability on a senior figure serves political purposes. It reduces the scope for questions about operational performance, instead lending itself to general queries of policy over which the head of an organization would have daily control. It also restricts knowledge flows to a single stovepipe that can shape the information shared with others. Moreover, it preserves the impression of the intelligence machinery as a closed environment beyond public scrutiny. The ISC has tried unsuccessfully to challenge this understanding and question mid- and lower-level officials about the United Kingdom's conduct during the war on terror period. The government's refusal to allow this led the ISC to conclude that they could not provide a full and rigorous scrutiny of intelligence policy and practice.[13]

In oversight forums, the agency head will normally defend their budget, explain their implementation of policy, deflect criticism, and jockey for more powers, but the efficiency of their organization (and particularly their effectiveness) is a mystery. While this preserves the secrecy of the intelligence environment, it reinforces a sense of distance between the agencies and the society they are protecting. The result is a limited dialogue, which inhibits the free exchange of ideas and information that might test orthodoxies and propose new ways of understanding and doing intelligence work. Nor is it straightforward to see such accountability gaps being filled by the executive. Ministers, who are supposed to oversee agency activities on behalf of the general public, are unlikely to challenge prevailing assumptions since they set the policy and so are implicated in operational decisions.[14]

Elite accountability carries with it some advantages that could serve the public good. For instance, it offers an opportunity for senior intelligence managers to reflect on their own policy assumptions and test them against informed commentators—within narrow parameters. The requirement to construct a narrative that rationalizes, explains, and justifies their existence and behavior to others cannot help but compel reflection—even if the narrative they present is not necessarily a true reflection of their self-identity or a full picture of their activities. Separating those who are undertaking intelligence activities from those who are meant to judge their rightness could also be useful—allowing clear lines of responsibility and blame, with the caveat that in doing so it may reinforce an "us and them" mentality, obscuring the fact that the agencies and the scrutiny bodies are all supposed to be acting in the wider public interest.[15]

Nevertheless, if elite accountability inhibits proper analysis of the performance and internal norms of intelligence organizations, this is problematic, as it means much of their daily activity is beyond scrutiny. A number of other factors also limit the range of "account-giving" in the intelligence context and mean that the concept is often understood in narrow ways. These include secrecy, limited organizational knowledge, legal controls, the separation of the domestic and foreign spheres, and the tendency to focus on retrospective punishment rather than learning.[16] These will be analyzed in turn before considering why accountability is important, who should conduct it, and what it is meant to achieve.

Limitations on Intelligence Accountability

Secrecy presents a problem for accountability because it seems to act in tension with the aims of the latter. Secrecy is about restricting knowledge flows and maintaining an informational advantage over rivals, whereas giving an account—especially if it is public—inevitably means sharing information and thereby reducing the mystique of an organization and its working practices. In some senses, changes to intelligence practice in recent years have made accountability and secrecy more compatible. Western governments have widened the ring of secrecy to enable a much greater range of agencies and officials to access intelligence since 9/11, to the extent that Richard Aldrich and Christopher Moran estimate "in the United States, over 5 million people enjoy security clearances."[17] In an effort to avoid the "silo thinking" that supposedly prevented connections being made that might have stopped the 9/11 terrorist attacks from happening,[18] there is now a much denser matrix of cooperation and dialogue between agencies. Similarly, in the United Kingdom, Alex Younger, the chief of SIS, has argued: "the key point that sets us apart as an intelligence community is our ability to work together. We have powerful but distinct capabilities. We are able to succeed through our ability to fuse them together, to become far more than the sum of our parts."[19] The corollary of this is that organizations have far more scope to give accounts of their behavior and open up their actions to scrutiny by peers and colleagues than in the past.

Yet the unintended effects of these policies have contributed to what Aldrich and Richterova term a "crisis of secrecy," pitting accountability and secrecy against one another once again.[20] The sheer number of people privy to secret intelligence has resulted in "ambient accountability," whereby wrongdoing is more easily exposed and "Disgruntled officials can now harvest and release entire archives of secret material with a pen drive."[21] Technology has thereby enabled more secrets to be collected but at the same time made them less secure as they are more easily shared. In response, governments are now deploying technology to identify in advance who might be "pre-leakers"—those liable to be future whistleblowers.[22] Yet in doing so they may be stigmatizing morally conscientious workers whose removal would narrow the scope for ethical challenge and debate within the organization. In short, secrecy and accountability remain in tension, and secrecy and technology may in the future combine to reduce accountability.

Secrecy does not only make account-giving and receiving difficult, but also makes it harder to evaluate the accuracy of those accounts. This applies both to the specific information relayed and the wider institutional context. Lack of organizational knowledge and information is an important and linked factor preventing external bodies from gaining a detailed picture of what really goes on within the intelligence services. In the U.K. context, the various commissioners expressed a desire in their reports to understand the organizational culture of the intelligence agencies and get a sense of their bureaucratic norms. However, these efforts were very impressionistic. The Intelligence and Security Committee (ISC) is said to have tried to focus more on effectiveness rather than just democratic control and propriety.[23] Yet this has been a slow process, partly due to its external institutional position: for all the selectivity of its membership and reporting, it is made up of parliamentarians—not current or former intelligence officials. Coupled with its limited resources and powers (albeit bolstered by reforms in 2013), and opportunity to talk only to agency heads, it has struggled to dig deeper into operational performance. When the ISC does comment on matters such as resources, IT systems, and buildings, this has been dismissed as little more than acting as "management consultants for the government" rather than being a rigorous source of critique on intelligence practices.[24] The U.K. intelligence machinery has been more open since it was put on a statutory basis, but practitioners and scrutineers are bound by the Official Secrets Act, and the numbers of people employed, even with its expansion, is quite small, totaling 17,331 in the main agencies, according to the most recent figures.[25] Therefore, few commentators have actually worked with or for these organizations, and those that have are not able to speak freely about how official narratives compare with their experiences.

The limitations of the ISC's membership are exacerbated by the technological advances affecting intelligence work. Data collection software and protocols require considerable technical knowledge to understand. Although ISC members have tended to have experience in the broad security field, as junior foreign or defense ministers, or academics, they are unlikely to have the technical background to allow a detailed evaluation of the implications of how agencies use technology in intelligence work—something exposed during the Snowden revelations.[26]

Legal mechanisms of accountability provide a higher level of control; however, in the case of the intelligence services this is qualified by the demands of national security. In the United Kingdom, the agencies operate on a statutory legal basis—with the Secret Intelligence Service governed by the Intelligence Services Act 1994 and the Security Service by the Security Service Act 1989. There are also important legal means of redress against these agencies, such as the European Convention on Human Rights and the domestic Human Rights Act 1998. Yet judges have been reluctant to rule against governmental policy made on national security grounds. In the past they have questioned the legality of some counterterrorism measures such as control orders (whereby individuals had restrictions placed on their movement and communications), but the decision to derogate from Article 5(1) of the European Convention relating to the right to liberty of terrorist suspects (on the Article 15 basis that the United Kingdom faced a "Public Emergency which Threatens the Life of the Nation") was described by a senior judge as "a preeminently political judgment" and so outside their expertise.[27] Similarly, the policy of bulk data capture—where agencies collected communications data from the entire U.K. population of users—has not been criticized by courts in principle, but rather in terms of practice.[28]

The distinction between judicial and executive control is challenged by the reforms of the Investigatory Powers Act 2016. By introducing judicial commissioners, who must make a judgment about the necessity and proportionality of warrant requests to search communications data or conduct surveillance, the act blurs the lines between judicial and executive aspects of accountability. The risk of this change is that moral and political elements of decisionmaking may be downplayed in favor of technical discussions of whether activities comply with the letter of the law.[29] Although evaluating necessity and proportionality would have to include some consideration of these elements, this would be done with reference to legislation and could marginalize wider public interest concerns. Furthermore, it is notable that the advisory notice explaining the commissioners' approach to approving warrants states: "On certain issues, such as, for example, what counts as legitimate ways to achieve foreign policy or national security priorities, the judicial commissioners' reviewing role will be necessarily limited and the judicial commissioners will afford a very wide margin of judgment to the secretary of state in determining such matters."[30] Overall, putting the secret agencies on a statutory basis and giving the judiciary a greater role in determining intelligence activity has increased the breadth and depth of account-giving. In that sense, accountability has been strengthened. Yet this operates within defined parameters and downplays important political and ethical questions about what is right and appropriate in favor of what is legal.

Another factor delimiting accountability in the intelligence context is a tendency to separate the domestic and foreign spheres. Activities within the former are subject to greater controls, while the latter can often enjoy remarkable freedom from scrutiny and auditing. For example, intrusive surveillance operations in the United Kingdom by British intelligence and security personnel require a ministerial warrant, yet abroad they are grouped as class authorizations under the Intelligence Services Act 1994. The Intelligence and Security Committee has noted that "agencies do not all keep detailed records of operational activity conducted under class authorizations."[31] As such, close scrutiny of the appropriateness of individual cases abroad is not possible. Similarly, in the United States the political controversy over Edward Snowden's revelations about bulk data collection centered on the idea that in spying on the communications of foreign individuals, the U.S. government was collecting the private messages of U.S. citizens as well.[32] This was seen as contrary to the Foreign Intelligence Surveillance Act of 1978, which required a warrant for surveillance on U.S. citizens. In other words, different standards and expectations of accountability apply, depending on where the activity is taking place and against whom.[33]

The final factor constraining intelligence accountability is the fact that it is almost entirely retrospective. The combination of a closed, secret system, little attention to internal standards and behavior, and a focus of scrutiny on the domestic realm means that intelligence accountability has tended to be centered on "firefighting"—that is, responding to flagrant breaches of standards or intelligence failures that emerge from either whistleblowers, policy errors, or surprise attacks.[34] Day-to-day "police patrolling" activities by scrutiny bodies like the U.K. Intelligence and Security Committee have been seen as flawed thanks to misleading accounts provided by officials (see chapter 2)—even when this body was made up of prime ministerial appointees and its reports could be heavily redacted to avoid compromising operations. Levels of "responsiveness" and interest in "providing answers" that are accurate tend to depend on wider public engagement in the media or via court processes—what Richard Aldrich terms "regulation by revelation."[35]

Such scrutiny is likely to be more confrontational and provoke defensive responses. It is also arguably damaging to the spirit of accountability overall, as it conflates account-giving with punishment. (In the United Kingdom, punishment does not usually take the form of dismissal or criminal prosecution but rather negative publicity, reputational damage, and political embarrassment—what Mark Bovens has labeled "face consequences.")[36] While the capacity to punish is a factor in any effective system of accountability, there has to be more to giving accounts than anticipating public censure—otherwise, the tendency will always be to avoid presenting a full narrative that acknowledges errors and allows genuine learning. As Glenn Hastedt notes, during and immediately after crisis situations, "the learning capacity of leaders and organizations is low" and so focusing accountability on events like these means that it is likely to be ineffective at improving future behavior.[37] Furthermore, since this form of accountability is retrospective, it is rather too easy for agencies to say that lessons have been learned, personnel have moved on, and that particular mistakes could not be repeated. It is also important to note that as the current oversight system in the United Kingdom does not allow whistleblowers to provide accounts to external bodies, with the possible exception of the ISC, individuals outside the agencies can only respond to concerns once they have become public via the media.

The introduction of judicial commissioners approving warrants (for domestic surveillance) does, for the first time, provide an element of real-time accountability, since this is supposed to be undertaken prior to the warrant being executed. If a warrant is required as a matter of urgency, and there is not time to gain judicial assent, the agency must report this to a judicial commissioner, who has to make a judgment within three working days as to its appropriateness and can cancel the warrant and order the destruction of material obtained.[38] Most processes of account-giving are retrospective as a matter of course, however. As noted above, the ISC explicitly excludes ongoing operations from its scrutiny.

In summary, accountability in the U.K. intelligence realm is restricted, elite-focused, largely retrospective, punitive (in terms of reputational damage), focuses on policy more than practice, and applies different standards of scrutiny depending on whether the activity is perceived as within the domestic or foreign spheres. This approach is driven by the imperative of secrecy and designed to minimize disruption to the work of the intelligence agencies. It assumes a high level of integrity on the part of officials and provides minimal oversight from the judiciary (except when it comes to warrants), legislature, or wider public. While executive approval is required for legally or politically sensitive operations, the extent to which this constitutes accountability in terms of oversight is clouded by the fact that ministers set policy. An example of confusion in this regard is apparent in the former British Foreign Secretary Jack Straw's attempts to deny knowledge of rendition operations allegedly facilitated by MI6 during his tenure. News reports suggested that officials paid him a visit and reminded him that he had signed off on these actions and so shared responsibility.[39]

Why Is Accountability Important?

The most obvious reason for concern over accountability is that organizations that are closed to external scrutiny are more open to abuse.[40] As Michael Andregg puts it: "Power tends to corrupt even the most open system; secret power systems and the people in them are especially vulnerable to this. Hubris corrupts all professions."[41] This is often highlighted as a danger to society, but it is also important for the intelligence organizations themselves. Ineffective accountability allows individuals the freedom to subvert organizational norms and standards.[42] This can manifest itself in a number of ways. At the collective level, officials may lose sight of the wider public good and seek to advance organizational goals—even where they conflict with the public interest. Tim Weiner has suggested that CIA officials during the Cold War "were prepared to lie to the president to protect the agency's image."[43] Alternatively, they might breach organizational norms where they perceive them to be an obstacle to wider public safety. The same author cites the CIA's deputy director of plans, Richard J. Bissell, as saying: "Many of us who joined the CIA did not feel bound in the actions we took as staff members to observe all the ethical rules."[44] Ian Cobain has alleged that the U.K. intelligence and security agencies continued to use the "five techniques" to interrogate Northern Irish detainees suspected of terrorism despite explicit prime ministerial orders to suspend the practice.[45] In some of these instances, the officials might not be acting in bad faith as such, but rather interpreting their priorities according to their own perception of operational requirements, in ways that may be unethical but are unchecked in the accountability vacuum.[46]

A separate set of problems comes from those who are motivated by individual rather than collective goals. Favoritism, bullying, paranoia, a focus on pet projects rather than collectively important tasks, personal aggrandizement via empire-building, and rent-seeking can all flourish in bureaucracies without external scrutiny.[47] In addition, individual ideological motivations can subvert collective norms—as in the case of double agents, coup plotters, or obsessive mole-hunters.[48] Peter Wright's role in MI5 as a counter-espionage operator combines all three elements, and Stella Rimington's account of the disruptive effect of this individual on the Security Service's performance is illustrative:

> by the time I knew him he was quite clearly a man with an obsession and was regarded . . . as quite mad and certainly dangerous. . . . He was self-important, he had an over-developed imagination and an obsessive personality which had turned to paranoia. And above all he was lazy. . . . It was hard to explain why he was allowed to stay for so long . . . He used to wander around, finding out what everyone was doing, taking cases off people, going off and doing interviews which he never wrote up, and then moving on to something else, while refusing to release files for others to work on.[49]

Having exhibited excessive levels of trust in officials and low accountability prior to the discovery of the Cambridge spy ring, the U.K. intelligence services would move to becoming "very inward-looking and to be extremely anxious about whether they had got traitors within their organization."[50] Mistrust permeated the organizations with consequent effects on efficiency, staff morale, and cohesion. One former SIS officer noted "a pervasive lack of institutional self-confidence" for decades afterward, which was "quite something when you consider how far back Philby actually was."[51] The risk in responding to failures of accountability is that it might lead to "accountability ping-pong," with formerly lax oversight becoming far more restrictive and burdensome before eventually having to be loosened again, something often seen as a feature of the intelligence field.[52]

Concerns that bureaucracies are acting beyond their powers or avoiding scrutiny are common, in one form or another, in many organizational contexts, but are particularly problematic in the intelligence realm because of the nature of that practice. Intelligence officials engaged in espionage are breaking the law—even if it is usually the law of a foreign state. Agents have to intentionally deceive others, at times spreading misinformation, falsely representing themselves, and offering commitments they may not be able to fulfill. Eliciting information via interrogation, coercion, or exploitation will routinely entail the manipulation of an individual to serve a purpose that will go against that individual's interest. Such methods are not the entirety of intelligence practice, but they are an important component. Even intelligence fields such as signals intelligence (SIGINT), which do not involve direct person-to-person contact, entail observing individuals without their knowledge and prying into their personal lives in ways that are deeply intrusive and would be seen as voyeurism in other contexts. As a result, a significant amount of the work of these agencies involves behavior that is contrary to normal ethical codes.[53] The pressures of such work on the moral sensibilities of practitioners are considerable. Accountability has the capacity to enable a twofold process of keeping individuals in these agencies honest as well as reassuring them that their behavior is in accordance with the public good.

Academic commentators have tended to portray the U.K. national intelligence machinery as historically cautious and wary of overreaching its power or undermining democratic processes domestically.[54] David Cameron complains in his memoirs that SIS, along with the military, was "a huge source of frustration" on Syria in their reluctance to propose options for covert action.[55] Richard Aldrich and Rory Cormac suggest that SIS refused to cooperate with mooted prime ministerial plans to assassinate foreign leaders on at least two occasions in the postwar period.[56] Meanwhile, Harold Wilson's cabinet secretary in the 1960s, Burke Trend, is said to have "gasped in horror at the thought of probing the private lives of MPs" when urged to do so by the paymaster general, George Wigg.[57] Clearly, the record is mixed, and there were instances of overbearing behavior, but it is interesting that SIS and the Security Service expressed concern at the "confusion over lines of ministerial accountability" that Wigg's muckraking activities for Wilson had wrought.[58] Given the lack of oversight in this period, there had to be an element of self-restraint on their part; otherwise their presence in public life would surely have been much more intrusive.

From a practical perspective, even if these agencies can somehow preserve their virtue without external pressure, they will struggle hard not to become sclerotic or irrelevant. Organizations that avoid rigorous external or internal review risk atrophy.[59] Therefore, it is in the agencies' own interest to have their assumptions challenged and their behavior scrutinized so that they can root out bad policy, receive new and innovative ideas, and be confident they are operating effectively.[60] The dangers of a lack of rigor in intelligence analysis were brought sharply home by the Chilcot report into the United Kingdom's decision to participate in the invasion of Iraq in 2003. In addition to outlining the numerous errors in the assessment of Iraq's capabilities, the inquiry noted that "At no stage was the proposition that Iraq might no longer have chemical, biological, or nuclear weapons or programmes identified and examined by either the JIC [Joint Intelligence Committee] or the policy community."[61] Poor scrutiny by policymakers had combined with official myopia to entrench the assumption that Iraq possessed WMD, even as the evidence from inspections began to suggest otherwise.[62]

To overcome closed-mindedness in bureaucracies, Rascoff advocates a "risk management" approach to intelligence governance involving greater transparency and "rationality review" via cost-benefit analyses. Yet transparency presents self-evident problems for secret organizations.[63] Also, for all the popularity of a risk-management approach in current public policy thinking, it can be problematic. Risk is not an objective category—in fact, done properly, risk analysis acknowledges its subjective nature and is clear about the contingent nature of its assumptions.[64] Employing terms like "rationality review" conveys a sense of logical and dispassionate judgment. When it is coupled with the notion of a "cost-benefit analysis," we are presented with a depoliticized, mechanistic process when the reality is far more complex and highly political. Nevertheless, Rascoff's proposals are important if only because they begin to break down the wall between organizational performance and external scrutiny bodies, opening up a space for internal account-giving to be incorporated into the overall system of accountability.

In short, contrary to much of the emphasis in academic and policy circles on accountability as important for democratic control, the above discussion has highlighted some of the organizational and operational benefits that it can provide. Internal account-giving—rendering internal accounts—can reinforce organizational norms, allow reflection on performance and learning for the future, highlight malpractice, and promote innovation. To ignore or downplay these processes and only focus on external mechanisms of account-giving—holding to account—is to present an incomplete picture of intelligence accountability.

Who Should Hold Intelligence Agencies to Account?

Advocating transparency and reviews begs the question of who would be able to supply such an appraisal. Current practitioners may be too close to the agencies to give objective commentary; former practitioners or retirees might be out of touch with modern methods, tools, and norms; peer reviewers from foreign agencies would not share the cultural awareness of why things are done the way they are; meanwhile, parliamentarians may not have the technical expertise to understand and critique the use of technology.[65] Anyone given access to sensitive material would have to undergo a substantial vetting process that itself might contain the seeds of unconscious bias toward those of a sympathetic mind-set.

In other words, intelligence accountability forums face a "legitimacy-accountability paradox." There is a trade-off, whereby those most able to judge the effectiveness of these organizations (through their knowledge and experience) are also those least likely to be seen as legitimate scrutinizers by third parties, because of their status as "insiders." Conversely, those more obviously independent and resistant to in-group pressures and socialization within government, such as members of nongovernmental organizations, the media, and citizen groups, are also most likely to be perceived by the agencies as either ill-informed, partisan, or potential security threats, and so are unlikely to be offered fulsome and accurate accounts of agency activities.[66] Having informed experts with prior experience scrutinize the agencies can make their conclusions more authoritative, even if activist groups might question their independence. As Jonathan Simon stated in relation to investigatory commissions: "The fact that typical commission members have already given distinguished government service of some sort is less a guarantee of independence . . . than an assurance that the speaker is the sort of person whose criticism is to be taken seriously." [67]

Yet the risk in asking former grandees to hold intelligence agencies accountable is that they will be unable or unwilling to question intelligence activities from first principles and do the necessary digging to expose malpractice. Loch Johnson has pointed out that in the United States "None of the major intelligence abuses that came to light during the 1960s and 1970s were uncovered by institutions of accountability inside the executive branch, but rather by media and congressional investigators."[68] The same applies to the United Kingdom.[69] As noted above, it was activist groups, academics, and the media who first brought to public attention the United Kingdom's involvement in rendition and policies on bulk data capture.

In the absence of effective scrutiny, it is perhaps surprising that abuses of power are not more common. Scholars have explained this as a result of the continual and important constraining effects of internal organizational norms that serve to check the abuse of power and hold personnel to account via the judgment of their peers.[70] Here, logics of appropriateness govern behavior and shape the accounts offered.[71] Yet it is just such forms of account-giving that are largely excluded from current accountability reforms and much academic commentary. If it really is these mechanisms that are most important to curtailing widespread abuse, then they deserve far more attention than they presently receive. Opening them up to scrutiny is vital, because maintaining a closed culture with very rigid norms is only likely to make accountability more difficult in the long run. The tendency will be for officials to close ranks to enforce group loyalty. Thus, the abuse of power may be more widespread than we realize, but group cohesion is preventing such information from coming to light.

Given these concerns, commentators from outside the intelligence community tend to favor more rigorous scrutiny by external bodies; however, that may be due to there being different "epistemic communities" at play. Academics see wider dissemination of knowledge as more conducive to collective learning and discovery. But in the realm of national security, such a move carries risks. Most obviously, there is the potential for security breaches as the circle of those privy to secret information widens to individuals who have not been vetted as systematically, may not be as adept at maintaining security protocols, or who cannot be sanctioned in the same way as an official with a career and a pension. If the individual scrutinizer is part of the legislature, there is a serious risk of political grandstanding.[72] This can be aimed at privileging a rival organization, furthering their own career profile, or, often linked, at using accountability mechanisms to attack the executive. The roving inquiry into Hillary Clinton's role in the death of the U.S. ambassador to Libya in 2012 carried strong implications of such behavior.[73]

These sorts of manipulations of accountability generally corrode public trust without benefiting the public good, because they are designed to further a sectional or individual interest rather than improve performance. Their focus tends to be more on punishment and humiliation of individuals than organizational learning and adaptation. Even when external observers are acting in good faith and with diligence, their lack of experience in the practices they are scrutinizing can create difficulties due to a lack of awareness of what is normal and what would be a breach of etiquette—as well as how operational demands may impinge on effectiveness. An example in the U.K. context was Lord Hutton's failure, in his inquiry in 2004, to appreciate just how unusual it was for the prime minister's communication staff to be handling intelligence material, working closely with the Joint Intelligence Committee in producing reports, and having a say in their presentation to the public.[74]

This leads us to consider the role of the media in soliciting information from the intelligence machinery and holding it to account. Claudia Hillebrand notes three ways in which the news media contribute to oversight of the agencies and can thereby link to accountability. First, they operate as an "information transmitter," bringing to light information on intelligence activity to the wider public.[75] The general public knows far more about what is done in their name thanks to coverage of intelligence stories, the reporting of leaks, and recording of criminal cases. Second, they can operate as a "substitute watchdog,"[76] uncovering evidence of possible wrongdoing and questioning the executive when formal oversight bodies fail to do so. In addition, they play a legitimizing role for the intelligence services, reporting their successes and offering them a means to communicate with the general populace.[77]

The media's role in holding governments to account is problematic, however. In the United Kingdom, scrutiny has historically been hampered by the blanket refusal by agencies and ministers to respond to media queries on intelligence. Thus, in response to a story in 2014 that the government was harvesting private information on users of the smartphone app Angry Birds, as well as Facebook and YouTube, GCHQ stated: "It is a longstanding policy that we do not comment on intelligence matters."[78] While the official "no comment" policy is a useful way for the agencies to avoid awkward questions, it also means that the agencies have not historically been able to refute erroneous reporting or laud their successes publicly—though plenty of informal tip-offs and briefings have been proffered to selected journalists.[79] Thus, the media's ability to act as an information transmitter is limited. The existence of the "D notice" system also constrains how much intelligence information the media communicates to the public.[80] Now termed DSMA (Defense and Security Media Advisory) notices, these are a mechanism by which newspapers clear certain stories with the intelligence and security agencies before publication to ensure they do not risk national security or public safety. Some newspapers have avoided using the system at times, to ensure that sensitive stories were not blocked, as when the *Observer* published a story on United Kingdom spying on the United Nations in 2004 and the *Guardian* published its first leaks from Edward Snowden.[81] But it is generally upheld and so acts as a barrier to full public disclosure of intelligence stories.

The U.K. media's capacity to act as a substitute watchdog has been significantly eroded in recent years due to the nature of the business environment it inhabits. Traditional print media are facing severe budgetary constraints as a result of declining readership and advertising revenue—in part, thanks to the advent of online and new social media. That means that lengthy news investigations into intelligence matters are increasingly burdensome. The kinds of stories that will "make" are likely to have an emphasis on novelty and contain a strong element of human interest. Thus, long-running issues struggle to compete for public attention and gradual changes over time—particularly structural or systemic ones—are unlikely to be reported.

While there are still some newspapers of record that can be consulted by the public, there is a massive array of internet news traffic, which can drown out more nuanced narratives. Important matters of context and analysis are often lost. In addition, there are actors who use these forums for ideological purposes. Groups such as Wikileaks are regularly criticized for publishing secret information without due concern for the safety of individuals listed in their data dumps.[82] The exposure of the full range of communications between governments—and of the actions of soldiers, diplomats, and civil servants acting on their behalf—is often defended as giving the public the chance to be truly informed, but it also arguably has the effect of subverting government itself. If governments are unable to have private conversations, the result would be severe poverty of rigorous policy discussion and the curtailment of a huge amount of legitimate diplomatic activity. It would also attack the very notion of secret intelligence, since nothing could be secret and, as everyone is privy to the knowledge, it no longer carries the informational advantage associated with "intelligence."

It is important to note that these leaks tend to have an unduly negative effect on advanced democratic governments, whose systems are more open to scrutiny compared to authoritarian and/or less developed states (although Wikileaks' revelations about the Tunisian president Ben Ali's family business concerns were credited with contributing to the toppling of the regime and the advent of the Arab Spring).[83] Nevertheless, while their primary impact seems to be to foster a general distrust of intelligence, they do regularly provoke traditional accountability forums in Parliament and Whitehall into requesting accounts from agencies about their activities, if only to refute allegations.

More unequivocally negative are the concerted efforts by states such as Russia to exploit the proliferation of media outlets in the West and promote disinformation.[84] In a speech he made in 2018, the director general of the

Security Service, Andrew Parker, described the problems hostile state activity in the online realm poses for the agencies and their efforts to inform the public:

> Age-old attempts at covert influence and propaganda have been supercharged in online disinformation, which can be churned out at massive scale and little cost. The aim is to sow doubt by flat denials of the truth, to dilute truth with falsehood, divert attention to fake stories, and do all they can to divide alliances. Barefaced lying seems to be the default mode, coupled with ridicule of critics.[85]

Parker lumps in media manipulation and social media disinformation with espionage and military force as part of a set of "hybrid threats" to the United Kingdom from Russia, in particular. Combined with the ideological agenda of anti-secrecy groups like Wikileaks, they represent a serious challenge to the ability of new forms of media to foster a constructive environment for account-giving. Of course, it is also important to note that the U.K. government exploited media interest in intelligence to justify intervention in Iraq in 2003—leading to misleading reports about national security threats. In doing so, it provoked greater skepticism about the veracity of intelligence reporting and the good faith of intelligence officials, creating a climate where government statements and media reporting could be challenged by, and given equal weight to, nonexpert opinion, especially in online forums. The U.K. government is therefore partly responsible for the decline in trust that followed.

When it comes to commentary on intelligence accountability, few authors consider the idea that the general public might play a role in holding intelligence and security services to account. The heads of the intelligence and security agencies gave evidence in public to the ISC for the first time in October 2013. They have also begun to speak to a wider audience in forums such as the RUSI,[86] intelligence symposia,[87] academic settings,[88] their own headquarters,[89] and even activist forums[90] in an attempt to explain their role and activities. In that sense, accounts are being given to the public, but the potential for the public to question and respond to these narratives is limited to the elite audience on each occasion. It makes sense for feedback on technical matters to be limited to an informed audience, but some of the issues that have troubled intelligence agencies in recent years relate to ethical questions that could benefit from public debate and scrutiny by lay people. For instance, when and how is it acceptable to use children as intelligence assets? Is it ethical for a government to "seek to alter the ideological views of its citizens as part of its counter-radicalization strategy"?[91] What kinds of response are appropriate to cyberattacks by hostile states? Should Western agencies be engaging in information warfare against authoritarian regimes? These are primarily ethical questions and as such are open to lay people to address.

Overall, the logic of commentary on intelligence accountability suggests that, internally, the agencies are best held to account by individuals with professional experience who can command peer esteem; meanwhile, external oversight is best conducted by groups who have demonstrable independence and rigor. However, each comes with risks and problems that resist easy resolutions. It is important to note that a genuinely unified system of accountability needs to provide clear mechanisms for internal and external account-"receivers" to talk to one another and share information so that a fuller picture of mistakes, inefficiencies, and immorality, as well as excellent performance and virtuous conduct, can be constructed. Furthermore, the sense that the public can or should be excluded from ethical decision-making in intelligence is unlikely to be sustainable and means that the intelligence community is missing out on a potentially fruitful source of innovation and legitimation.

What Is Accountability Meant to Achieve?

This leads one to consider what accountability is for. Intelligence scholars offer subtly different interpretations of its purpose. Maria Caparini sees it as about weighing the efficacy and propriety of the agencies' activities.[92] Ian Leigh opens up these categories and views it as potentially checking "efficiency or effectiveness, legality or proportionality."[93] In both, there is a division between assessing the technical performance of intelligence organizations and making a moral or legal judgment about their ethical or judicial status. A further school of thought draws comparisons between intelligence and the broad field of civil-military relations,[94] identifying the three themes of accountability in this sphere as democratic control, effectiveness, and efficiency.[95]

The latter group tend to be skeptical of the extent to which the effectiveness and efficiency of the intelligence agencies are—or can be—evaluated by accountability forums, especially those external to those organizations, and so focus on democratic control instead.[96] The implication of much of their writing is that accountability's true purpose is to ensure that democratic values and institutions are not being subverted.[97] The power that secrecy and a license to break the law (at least abroad) offers to intelligence officials is considerable, and so accountability is necessary to provide checks on this power and a means of redress for abuse. As a result, intelligence is depicted as an extreme example of the wider tensions in government, between technical expertise, bureaucratic power, and governmental surveillance on the one hand, and individual autonomy, civil rights, and democratic rule by an informed public on the other hand.[98]

In this sense, discussion of intelligence accountability links to the perennial "principal-agent" problem of how a governing actor (the principal) can achieve their goals when the individual or organization tasked with implementing their instructions (the agent) might have their own identity, beliefs, standard operating procedures, and interpretations that affect the result.[99] Thus, the main task of accountability would be to limit any inclination of intelligence and security agents to subvert the will of the principal—either by aligning organizational norms with the intentions of the principal (internal accountability) or providing public affirmation of the principal's instructions (external accountability). What complicates this further is there are at least two principal-agent relationships at play in any discussion of intelligence accountability.[100] On the one hand, the general public is the principal, delegating authority to the state (the agent) to provide for their security (with intelligence a vital component of this).[101] Public accountability is designed to ensure this is done appropriately and effectively. On the other hand, there is also a second-order principal-agent relationship between the government and the agencies. Here, the task of accountability is to ensure these organizations are not acting *ultra vires* (beyond their legally authorized powers) and are carrying out the instructions of the government. This includes acting according to the U.K. civil service code's expressed values of integrity, honesty, objectivity, and impartiality, meaning that officials do not "frustrate the implementation of policies once decisions are taken," or "deceive or knowingly mislead ministers, Parliament, or others."[102]

In devising any system of accountability to cover one or both of these, there is a dilemma over how much autonomy should be afforded to the agent. Governments have to make decisions in secret to avoid handing their opponents an advantage, but this also creates scope to act against the public interest without the public being aware or able to seek redress. There is an argument that officials should be allowed the freedom to use their expertise, knowledge, and judgment to act effectively. This frees agents to use their initiative, but it might also provide a permissive environment for abuse and reduces executive oversight. A balance has to be struck between autonomy and control. Here, secrecy constitutes a substantial obstacle to judging what is appropriate, as principals may not have a full picture of the facts and so could hamper performance, either by being overly restrictive and crippling innovation or by being unduly deferent to expertise. For many practitioners, the need to maintain secrecy trumps the risk of minor performance errors, and so accountability is only intended to avoid the most egregious forms of malpractice—in terms of waste of public money, corruption of political processes, or endangering public safety.[103]

Instead of seeing accountability merely in terms of negative control, it is possible to see it in more positive terms. Viewing accountability as about account-giving and -receiving, rather than "being held to account," we can begin to see practical benefits for all sides. For example, giving an account and receiving feedback offers an opportunity for organizational learning and changes in behavior that might prevent the repetition of mistakes and improve performance. The act of devising an account compels reflection and rationalization of behavior, reminding the official why they are acting, in whose interest they are supposed to do so, and what the boundaries for action are. Thus, the account-giving process reinforces professional norms and links them to the values of the wider society they are seeking to protect.[104] Such accounts could also foster group cohesion by reinforcing a self-identity of a law-abiding and respectable entity acting in the public interest. In this way, it enhances the internal workings of the organization as well as promoting its reputation externally—what Geert Bouckaert and John Halligan describe as "The legitimizing capacity of a good performance story."[105]

The latter point is important, because legitimacy is such a vital aspect to intelligence work.[106] Public trust in the security and intelligence services is essential to many of their key duties, such as counterterrorism, which relies on the cooperation of communities for intelligence-gathering. In communicating the purpose and nature of their activities to scrutiny bodies, accountability can help to reduce tensions between the intelligence services and those communities who are subject to intelligence operations. By offering an account of how and why they are acting, intelligence officials can demonstrate the links between their actions and public goods like community safety and cohesion that benefit those groups as well as wider society.[107] Although the exposure of wrongdoing may affect public trust in those organizations, the overall system is reaffirmed when those who are responsible are visibly asked to account for their behavior and demonstrate how it aligns with the collective good of society.

Similarly, although the technical means of redress that accountability offers might seem to lead to negative publicity, in the long term there are net gains for those organizations in terms of efficiency. By exposing when agencies have broken legal rules, performed inefficiently, been ineffective, or failed to advance the wider public good, accountability regimes allow them to correct their own behavior and improve their performance as a result.

That said, if accountability is to be useful, it should also include scope for offering examples of good practice that other agencies might follow—and have the capacity to reward excellence as well as punish malfeasance.[108] That suggests a more transcendent system of accountability—one that permeates the agencies and operates at multiple levels. Such a move would challenge the tendency to see accountability as a negative activity.[109] It may also move it away from simply being a retrospective process.[110] Rather than accountability as a "response" or "answer," it might begin to be a process of dialogue between the account-giver and -receiver that offered a route to real-time innovation and correction.[111]

To summarize, control is only one of a number of rationales for accountability regimes. Accountability is also an important means of improving the performance of individual officials, upholding collective standards, checking the appropriateness and effectiveness of behavior, and adapting policy in light of the challenges facing those receiving the account. Yet there are difficulties in the account-giving process due to the nature of the work of the intelligence agencies. If secrecy is vital to what they do, simply calling for more openness and transparency is trite and ignores the risks this creates for the public good. Of course, the flipside is that if these agencies are like other governmental bureaucratic organizations (and there is no reason to suggest they are not), secrecy and a lack of accountability at the operational level comes at a likely cost in performance.[112] In the absence of rigorous, open debate, assumptions can become ingrained and bad policies pursued without proper checks or challenges.

The task then is to create a system of accountability for the intelligence services that allows them to function but also ensures their activities are in accordance with domestic values and are performed efficiently and effectively. The logical method of doing so is to accept that some forms of account-giving are necessarily internal and secret, but acknowledge their existence and demonstrate how they link to external and public accountability forums to provide a more holistic system.

New Accountability Challenges

A further difficulty of viewing accountability in terms of control is it implies a linear model of policymaking. The idea of civil servants accountable to ministers, who are in turn accountable to Parliament and ultimately the electorate, fits closely with the Whitehall/Westminster–focused models of governance that traditionally dominated analysis of British government and politics.[113] It suggests a delineable set of policy actions and outcomes, with clear lines of agency and responsibility. In reality, as numerous studies of governance in the United Kingdom have demonstrated, policy neither originates nor is implemented in such a hierarchical fashion. Instead, it is far messier, with policy initiatives emerging across government and the private sector, and at various levels of institutional hierarchies. There is also a strong transnational element to policymaking. Decisions may originate from other actors globally, or through interaction between domestic and international actors, and the way they are implemented is shaped by transnational legal and political arrangements. Thus, governance is "decentred" and the state is fragmented, since a plethora of actors decide, interpret, implement, and contest policy.[114]

It could be argued that intelligence is different from normal policymaking, as secrecy means that the executive retains control over much of the policy process. Yet secrecy also carries the potential to obscure the practice of intelligence from other tiers in the hierarchy. Moreover, thanks to technological advances in digital communications and surveillance, a far greater number of agencies within government now produce and consume intelligence. That means a denser and broader network of intelligence practice. Intelligence cooperation with other states has also widened and deepened, particularly as part of global efforts to combat terrorism, supported by international agreements, such as UN Security Council Resolution 1373.

Therefore, our understanding of accountability should perhaps move away from linear understandings of control and instead reflect the reality of a more dynamic intelligence policy environment. Focusing on how accounts are rendered, via processes of account-giving and -receiving, rather than just lines of management responsibility, opens up our understanding of how intelligence is understood and practiced across government, and between U.K. government agencies and their counterparts abroad. It also encourages more creative ways to scrutinize this activity, beyond the narrow horizons of judicial or legislative oversight.

A second challenge to current understandings of accountability lies in the rapid and transformative impact of new technologies on intelligence practice. The human element of intelligence work, not just in terms of data collection but also analysis, is increasingly giving way to automation and artificial intelligence. Thus, analysis of internet traffic makes use of algorithms that search for predefined behavior likely to indicate criminality or security threats.[115] Importantly, artificial intelligence is also coming into play in this regard, with machines learning and adapting to feedback in ways that go beyond the original human-derived parameters. A 2018 Chatham House report sets out the impact of this shift:

> For all of human history, politics has been fundamentally driven by conscious human action and the collective actions and interactions of humans within networks and organizations. Now, advances in artificial intelligence (AI) hold out the prospect of a fundamental change in this arrangement: the idea of a non-human entity having specific agency could create radical change in our understanding of politics at the widest levels.[116]

A particular problem for intelligence accountability lies in identifying the responsible actor in each case. Thus, if suspect activity is wrongly detected and leads to serious human consequences, this may be caused by a machine that is unable to account for its actions. In addition, should this be the result of artificial intelligence, human operators may not have even been aware of the processes that led to the outcome and so can deflect responsibility, leaving the victim unable to seek redress.

To overcome this issue, commentators have advocated mixed human-AI arrangements, sometimes described as "centaurs," whereby "the machine can process enormous quantities of data quickly while the human can spot-check and correct where necessary."[117] But this might not be practicable, depending on the quantity of data involved and the complexity of the analysis undertaken. One of the hoped-for advantages of using technology was that it could eradicate errors caused by human prejudices; however, when artificial intelligence systems have been deployed to sift data and make judgments, they have been found to replicate the biases of human society.[118] Amnesty International and Access Now launched a declaration in May 2018 designed to protect the "rights to equality and non-discrimination in machine learning systems."[119] To overcome the potential biases in machine learning systems, the declaration advocates the "active participation of, and meaningful consultation with, a diverse community to ensure that machine learning systems are designed and used in ways that respect non-discrimination, equality, and other human rights."[120]

The problem lies in the fact that current official mechanisms of accountability are, as noted above, elite-driven, and as such do not reflect the diversity of the population at large. Meaningful consultation with diverse groups is not being undertaken in this area by the intelligence community (though some intercommunal dialogue occurs in other areas, such as over the PREVENT strategy). Moreover, since accountability is often conceived in terms of linear models of decisionmaking, leading to a retrospective punitive judgment, existing accountability mechanisms are ill-equipped to grapple with the nonlinearity of AI and other technological issues. If a fuller understanding of accountability was used, encompassing "rendering account"—account-giving—as well as "holding to account," this might open up space for dialogue between intelligence officials and cyber-experts from other fields, and a recognition that AI creates ethical dilemmas for producers and consumers.

A final category of problem for intelligence accountability, and one that is increasingly apparent, is whistleblowing. As noted above, technology and social changes have combined to make it easier to leak sensitive material and distribute it widely through online platforms. Perhaps the most infamous example for the United Kingdom was Edward Snowden's 2013 revelations about Britain's interception of communications data in cooperation with the United States. Yet despite this leak leading to three major reviews of intelligence practice and new legislation, it is curious that neither the reviews nor the Investigatory Powers Act that followed made any effort to reconsider the current procedures for whistleblowing. It has been disputed whether Edward Snowden is a whistleblower or simply a traitor for leaking secret intelligence; however, his actions undeniably led to substantial debate over intelligence practices. They also demonstrated the challenges faced by the agencies in maintaining secrecy—particularly when it comes to programs that involve interagency cooperation. In his first report, the investigatory powers commissioner argued: "in the post-Snowden world, the security and law enforcement agencies can no longer expect to work in the shadows, in the sense that material which can properly be made public should be widely available for scrutiny."[121] Thus, the commissioner seems to concede the public benefit that flowed from Snowden's actions.

The 2015 RUSI report did mention some of the internal procedures for staff to express concern about what they are asked to do. MI5, SIS, and GCHQ each have a dedicated ethics counsellor to whom (according to the report) "ethical concerns can be raised and discussed freely" by staff.[122] In addition, a staff counsellor is available to officials, described as "an external appointee who works across the three agencies" and who "is a point of contact for any members of the security and intelligence agencies who have anxieties relating to the work of their service which it has not been possible to allay through the ordinary processes of management or staff relations."[123] The staff counsellor's function was elaborated in a written statement by David Cameron in May 2016, as he appointed Julian Miller to the post: "The post holder is available to be consulted by any member of the Agencies regarding matters of conscience about the work of their service, or a personal grievance or other problem which has not been resolved internally."[124] The counsellor apparently produces reports on at least an annual basis to the prime minister and relevant heads of department.[125] The RUSI report also makes reference to a whistleblowing policy "by which employees can raise any concerns over perceived malpractice or impropriety" but does not elaborate on how this operates.[126]

The workings of these three mechanisms of account-giving have not been made public, with the exception of occasional stories related to concerns expressed by officials, as reproduced in the ISC's Annual Report in 2009.[127] They have also attracted academic criticism for being too close to management structures or, in the case of the staff counsellor, operating more as an "agony uncle" than a rigorous means of highlighting concerns and having them addressed in a way that might change policy.[128] The lack of transparency about the identity of the staff counsellor (with the exception of David Cameron's parliamentary answer in 2016) and their function, leaves an information vacuum, which does not serve to reassure the public that officials will be encouraged to raise concerns without repercussions for their career or safety. Important questions can be raised about their operation: should the counsellor maintain confidentiality to protect the source or do they have a responsibility to report wrongdoing? Is anonymity possible for those reporting concerns? Would it be enough to feed complaints up the internal chain of command, or, if the policy itself is wrong, should they communicate this to an external third party?

A further set of questions arise when it comes to how counsellors link with their internal and external counterparts. What right would judicial commissioners have to access any information provided to counsellors? Who holds judicial commissioners accountable if their approval of operations were to be reckless or wrong? In extreme cases of malpractice, when would an official be justified in circumventing these procedures and notifying scrutiny bodies, such as the ISC, their MP, or the media?

I explore the workings of the counsellor system in chapter 3 through interviews with practitioners. For now, it is worth noting alternative means by which whistleblowers are encouraged in other spheres. In recent decades, the United States has encouraged corporate whistleblowing in the finance world through a series of regulations and laws designed to "express a decidedly moral view of whistleblowers as allies in the fight against corporate fraud, bribery, and corruption."[129] This even went so far as providing substantial monetary incentives, such as the 2010 Dodd-Frank Act, which stipulated that whistleblowers could receive a proportion of the monetary sanctions imposed on those found guilty, with the average bounty expected "to be well in the range of $2 million to $5 million dollars."[130] In the medical profession, Chanel Watson and Tom O'Conner have noted that doctors have been investigated by the General Medical Council for not "blowing the whistle" and reporting poor patient care—indicating this is a professional duty that carries the threat of sanction or even dismissal if not fulfilled.[131] These are examples of strong regimes that incentivize whistleblowing but neither approach has been tried in the U.K. intelligence context. The nearest the intelligence and security agencies have come to embracing whistleblowing as an ethical duty was when Eliza Manningham-Buller, director general of the Security Service, issued a circular titled "Ethics and the Security Service" in 2006, stating: "I urge staff to say if they have qualms. The idea that airing concern on the proper channels risks damage to career is a myth."[132] Yet the reporting mechanisms at this time were largely in-house, and so it is hard to evaluate their effectiveness.

Organizations can often be resistant to change and become entrenched in their habits, at the risk of ignoring important warnings about the need to reappraise their actions. At times, it may take an outsider to offer the requisite level of detachment to look at patterns of behavior afresh and make a moral judgment about appropriateness against wider social values. As an example, Philip Zimbardo notes that in his infamous Stanford prison experiment in 1971 (whereby college students were assigned roles as prisoners and guards to see how far they altered their behavior to fit these positions) the participants began to engage in psychological and sexual abuse, but he and his fellow investigators were so wrapped up in their observations that they failed to stop the study until his romantic partner visited the facility and was horrified by the goings-on.[133] The question is whether the intelligence and security agencies have equivalent individuals in place to act as a moral check on their everyday practices. The staff counsellor is external to the organization, and so on that level they might be sufficiently detached to offer a fresh perspective on any activities reported to them—though to be appointed to this position they must have had some familiarity with intelligence and security work, and so would also have the status of insider compared with a lay person. They also appear to act more as a sounding board than an inquisitor.

Incorporating whistleblowing to external bodies within the official accountability framework carries its own risks. Individuals might raise complaints for egoistic reasons—to self-identify as mavericks or heroes in a corrupt system—rather than as a genuine effort to effect policy change. In the latter cases, it may be difficult or impossible to assuage the complainant's concerns, and trying to do so could undermine the overall efficiency of the organization. It also threatens the integrity of the secret intelligence system. Secrecy may be required for collective reasons, and individuals, unless very senior, will often hold a narrow personal perspective that prevents them from accurately judging what is safe to share with other parties externally. In that sense, whistleblowing could endanger colleagues' safety or even lives. One can also imagine recourse to external parties undermining the social fabric of intelligence agencies. Secret organizations rely on their members working closely together, exercising discretion and trust. That also arguably extends to offering colleagues the opportunity to correct negative behavior themselves rather than be compelled to by external actors. As Geoffrey Hunt puts it, whistleblowers are "caught in this contest of accountabilities—a hero to the public and a troublemaker, even a deviant, to the organization."[134] Yet, as noted above, "accountabilities are shifting, or can be shifted, to encompass a wider arena of stakeholders."[135] Senior officials are now giving accounts in public and to external bodies. If other members of the intelligence machinery perceive these to be inaccurate or misleading, they may feel a divided loyalty between their organization and the public interest. Furthermore, it is worth noting the personal costs of not whistleblowing. In other professions, this carries legal penalties and psychological costs to individuals' welfare.[136] Given the technological and social changes in intelligence work in the digital age, the intelligence machinery is going to need to give more attention to how it enables its staff to consider the ethical implications of their work and perhaps blow the whistle on malpractice and unethical policies in a safe manner. As will be seen in chapter 3, more space has been opened up to ethical debate and the expression of dissent among personnel, but there is still a lack of coherent avenues for whistleblowing.

Nor can this simply be resolved through legislation. In the United States, there is a relatively dense legislative framework to encourage whistleblowers and protect them from retribution, starting with the Intelligence Community Whistleblower Protection Act (ICWPA) of 1998.[137] Yet when an intelligence official followed the correct procedures in making a complaint against President Donald Trump in September 2019 through the inspector general for the intelligence community, the whistleblower faced a campaign of harassment and vilification. The president called for the person's name to be revealed on a number of occasions, accused the person of making up "false stories," and implied that he or she should face retribution.[138] The person's identity was also possibly leaked in a tweet from the president's son.[139] This is a reminder that the right political culture needs to be in place—one that acknowledges the public benefit of whistleblowing—if those who do so through the proper channels are to be protected.

To recap, from the above discussion it is apparent that the accountability of public bodies involves both soliciting information about their behavior and compelling them to explain and justify their actions. In the world of intelligence, these processes are restricted, elite-focused, largely retrospective, focus on policy more than practice, and apply different standards of scrutiny depending on whether the activity takes place domestically or overseas. The need for secrecy inhibits the space for account-giving as well as the range of people who would be suitable recipients of such accounts; however, there is more to accountability than just the formal structures of reporting. Accounts are shared, justifications offered, and actions judged within organizations, as well as across Whitehall and beyond, including public and private actors.[140] Therefore, organizational culture and wider social norms and practices come into play. In the following chapter, the accounts that have been solicited by formal accountability mechanisms will be explored and the issues they raise delineated. While an increasing level of formal scrutiny has offered a much richer understanding of what the U.K. intelligence and security agencies do, it also underlines the limits to such forms of accountability.