5 The rights of foreign intelligence targets

Michael Skerker

Liberal states are dedicated to the protection of human rights but protecting the rights of their citizens may entail infringing upon or violating the rights of foreign citizens. This is what some call the liberal dilemma of intelligence collection (Omand and Phythian 2018; Gendron 2005, 418). The same is true for military operations, but in many cases, wars are avoidable, at least in principle, through deterrence and diplomatic actions. Yet intelligence gathering, by its very nature, must be ongoing, in part to forestall wars. If a state can build weapons of war with a reasonable hope that they will not be used and train military personnel with a reasonable hope they will not be deployed, the same is not true for intelligence-gathering equipment and personnel.[1]

In what follows, I articulate a cosmopolitan model for just intelligence collection directing all states with a certain character to adhere to the same norms when and if they engage in intelligence collection. This chapter focuses on signals intelligence, SIGINT, and image analysis intelligence, IMAGINT. The model ultimately cautions states to be conservative in their intelligence-gathering efforts. All states of a certain character are permitted to engage in the most rights-respecting, most efficacious techniques they have at their disposal. Given the range of technical abilities of different states, a state with discriminate, sophisticated means of intelligence gathering must consider if its citizens can tolerate the cruder, less discriminate retaliatory operations an adversary state might employ.

Foundation for a theory of just intelligence

This section develops the foundation of a cosmopolitan theory of just intelligence collection. I develop it in detail elsewhere (Skerker 2020b; 2019; 2016). In brief, people living in groups have collective moral responsibilities to protect and address other people's rights that can only be consistently and reliably met through coordinated action. Typically, these collective moral responsibilities are partially acquitted by creating and supporting institutions to address the relevant rights, like schools, hospitals, businesses, churches and militaries. These institutions are essentially outcome-oriented, set up to foster, create and protect the collective moral goods (e.g. health, education, security) that protect rights and fulfil morally important needs. Once these institutions exist, the collective moral responsibility of laypeople is partly met by supporting these institutions.

DOI: 10.4324/9781003164197-8

The professionals who work in morally vital institutions meet their collective moral responsibilities in part by adhering to their properly constituted professional norms. Since these institutions are created to acquit collective moral responsibilities, professionals have a moral – and not just a professional or legal – duty to comply with their professional imperatives to accomplish their institutions' characteristic ends. The relevant duties are moral duties since actors' norm-guided actions help their institutions meet, foster and protect people's rights.

Professional norms are chiefly ends-oriented, directing the professional to take steps that bring about their institutions' characteristic ends for their clients: education, justice, health, security etc. Professional norms are also constrained by deontological concerns reflecting *ex ante* rules winning the hypothetical consent of all affected by the professionals' actions. These constraints specify how the institutional imperatives are to be met, guided by stakeholders' presumed aversion to being grossly wronged in some areas while being assisted in others.[2]

Professional norms

Certain state agents have a professional duty to meet the collective moral right of security for their political entities, but this duty is too vague to be action-guiding. We can take advantage of the criterion of universalizability inherent in most schemes of rights and duties to further delineate relevant professional duties. We can consider if everyone affected by a potential tactic or norm (norms can be seen as rules for generating tactics)[3] would endorse it for meeting their interests and protecting their rights. Those affected would include three stake-holding groups for any professional action in an adversarial field (like policing, soldiering, law, or intelligence): the professionals themselves, their "targets" and their clients. In the abstract, we can see that these groups would endorse tactics and norms striking an optimal balance between being practically efficacious and rights respecting for all concerned. Any member of the stake-holding groups can be expected to endorse professional norms and tactics that efficiently and reliably lead to the characteristic end of their professions like security, but in a way that minimizes rights violations along the way. This trade off can be expressed by the adage "the cure shouldn't be worse than the disease". The preferred moral framework I call the "security standard" identifies norms and tactics rationally worthy of consent by the three stake-holding groups. It endorses norms and tactics surviving a three-stage winnowing process. In the context of security-seeking professions, the standard 1) canvases locally feasible tactics aimed at securing an environment relatively free of rights violations or the threat thereof 2) isolates the most reliable, efficacious, proportional and efficient tactics of those locally feasible and 3) endorses the most rights-respecting among the tactics meeting the practical metrics of 2).

Before proceeding, let me address some potential methodological questions. Hypothetical consent is sometimes criticized for being inadequate to ground norms or obligations. I am not arguing that intelligence gathering norms are based on hypothetical consent. Rather, they are based on collective moral

responsibilities. The hypothetical consent of all stakeholders is modelled to delineate the contours of these norms. Hypothetical consent is also sometimes criticized as a theoretical flourish adding nothing to what a theorist happens to find compelling. A hypothetical consent model *is* apt for crafting norms for national security actors because the theorist cannot say ahead of time which kind of professional norms and tactics in the security sphere are best for all political entities in all times. There are two contingent variables affecting national security that have to be taken into account: available tactics and the current level of danger. The first element of the security standard canvasses locally feasible tactics. Best practices for certain kinds of intelligence operations will shift over time as technology improves, social science makes breakthroughs and tactical experience expands, so what is consent-worthy for being a state-of-the-art intelligence-gathering method one year may be outmoded years later. Agencies also develop insights at different paces, so state A's intelligence apparatus can be faulted for using relatively unreliable or ineffective techniques already abandoned by other states, provided that these better techniques are economically and technically feasible for state A. Thus, element 2 of the security standard seeks the most practically effective norms and tactics that are currently employed somewhere in the world, and demands, effectively, that our political entity practice the state of the art, or as close to it, as is technologically or economically possible for it (further, since the security standard endorses the best norms and tactics, it places constant pressure on state agents to refine their capabilities). A second reason that different norms and tactics might be consent-worthy in different states is that more aggressive security-seeking tactics or less deferential norms might be consent-worthy in times of great danger.

The clients of intelligence officers – the inhabitants of their state – have a positive right to security. Therefore, they can demand their agents deliver that security. Intelligence officers can model their clients' consent to the most efficacious norms and tactics to that end. Their concerns would not be limited to efficacy, but also take into account reliability and efficiency. Since any kind of professional action might also produce negative effects, proportionality is also important to consider. An intelligence officer has no rational grounds to think a generic client would endorse relatively ineffective, inefficient, unreliable and disproportionate norms and tactics when better ones exist. No doubt some techniques (or norms encompassing tactics and techniques) will be more efficient, but less reliable or more efficacious, but less proportionate etc. so we can imagine an overall net "value score" of these four practical elements answering the question "what norm or tactic works best". Still, the norm or tactic best conducing to security is not necessarily consent-worthy. Among a class of high-scoring norms or tactics, those that are the most rights-respecting are most worthy of consent on account of clients' duties to respect the rights of foreigners and their own intelligence professionals and because of clients' interests in being exposed to the least rights-infringing tactics on the part of foreign adversaries.

This rights-respecting element will itself be the product of an optimal balancing of the interests of the three-stakeholder groups. The client's positive right to

security will be largely met with practically efficacious norms and tactics that actually do conduce to protect security. These norms and tactics may have to be modified from the highest levels of efficacy or efficiency in deference to the rights of the targets as well as the state agents implementing them. While targets of given actions can also be the clients of the same actions when they are wielded by their own domestic intelligence agencies, qua target, their interest would be to be exposed to no intelligence collection. Barring that, their interest is in being exposed to the most minimal, necessary and discriminate types of collection, meaning that qua target, they would endorse the most reliable, effective, efficient and proportionate measures, infringing on as few as their rights as possible. Intelligence collectors should spend no more time or collect no more information than is necessary. When it comes to inter-state intelligence collection, it is in the interest of the client in one state to endorse the most minimal and discriminate actions targeting foreigners, because as we will see in the next section, she implicitly endorses those same tactics being used against herself by foreign intelligence agencies.

Regarding the third stake-holding group, state agents have a right not to be ordered to perform actions exposing themselves to wanton risk or threatening their long-term mental, moral and physical health (Skerker 2020a). For example, intelligence officers can probably never be ordered to have sexual relations with targets or to cultivate drug addiction in the course of undercover work.

Thus, acceptable norms and tactics may vary if we take into account rights and not merely the efficacy of the norms and tactics. They may also vary if the rights of all three stake-holding groups are taken into account as opposed to the rights of just one. Examples will be given in a later section. The triangulation of rights is in the interests of all since any given person might at some point occupy all stake-holding groups. A person might be a state agent for some span of her life; be targeted by a foreign intelligence agency and be the recipient of the security provided by other state agents.

Forfeiting, Waiving, and Ceding Rights

Just because an institutional actor has a duty to do something it does not mean she is not wronging her target/client in executing her duty in a norm-compliant way. For example, a doctor has a duty to preserve people's health and must adhere to certain norms and tactics balancing healthy outcomes with respect to patients' rights. Just the same, she may not examine someone in a non-emergency situation unless the patient consents. The patient's consent waives claim rights that would otherwise make it morally wrong for the doctor to touch or probe the patient's body. A previous section concluded that security standard-compliant norms and tactics will respect the rights of all three stake-holding groups involved with intelligence collection. We now need to discuss which rights these groups enjoy. We will focus on how targets and non-targets (whose information might be accidentally collected) might forfeit, waive or cede rights to adversary intelligence officers.

One temporarily forfeits certain rights when one acts unjustly and another party acting in self- or other-defence needs to materially infringe on those rights to halt the unjust action or threat. So, for example, an unprivileged irregular militant, bent on committing acts of terrorism, forfeits privacy rights to his operational communications if intelligence agencies need to intercept his communications in order to interrupt his plots.

Some intelligence targets like national security actors waive rights that would otherwise morally inhibit intelligence agencies from targeting them for collection. One might expressly waive a claim-right to another person, giving her a liberty-right to act in a way that would otherwise violate the rights of the person who ceded the right, as when a patient cedes a right to a doctor to touch his body. Service personnel arguably waive claim-rights against being attacked to future conventional enemies when they enlist in the armed forces, extending permission to enemy service personnel to try and attack them in war-time.[4]

Most non-targets of collateral intelligence collection do not waive their relevant rights. Some *cede* relevant rights though. Again, one can *waive* rights through express consent or tacit consent.[5] Ceding rights can come as part of being duty bound. A duty to deliver X to Y means one cedes a claim-right for X to Y. One could not, for example, object if Y took proportionate means to seize X if one did not voluntarily do one's duty and deliver it. One might have a duty to deliver something to someone in the context of a particular practice like a game, but more often, one has duties outside of particular practices one voluntarily enters.

One owes a duty to uphold just institutions to the inhabitants of a state and directly expresses the duty to the government employees who are those inhabitants' agents. A duty to uphold just institutions means ceding claim-rights against state agents 1) when those agents are competently pursuing their professional obligations and duties and 2) when insisting on those rights would prevent state agents from serving their principals. This ceding of claim-rights gives the state agents liberty-rights in turn, creating the space for them to perform their norm-compliant actions without wronging the affected parties. So, for example, domestically, a person's duty to uphold just institutions means he cedes claim-rights against having his liberty curtailed by competent police hewing to due process protocols in the event that evidence implicates him of a crime. One does not cede claim-rights to professionals acting in violation of their professional norms or incompetently executing their norms.

The duty to support just institutions is not restricted to institutions of one's own state, but extends in different ways to foreign institutions. The duty to support just institutions is based on the duty to protect the rights of other human beings, a cosmopolitan duty which is unaffected by the nationality of the recipient. So, for example, one cedes claim- and liberty-rights to the state agents of a foreign state one visits as a tourist when insisting on those rights would prevent foreign agents from permissibly performing their duties to protect their own citizens, residents and guests (e.g. tourists).

Normally, the duty to support just institutions does not require one to do anything for state B when one is residing in state A.[6] That said, one should usually

cooperate with foreign law enforcement officers if one can provide information about a crime committed abroad. This is an expression of the cosmopolitan duty to help protect other people's rights. The foreign law enforcement effort may also protect oneself in the case of international crime like drug trafficking or terrorism. This claim may not be too controversial. When it comes to another state's *adversarial* actions against one's own state, the duty to support just institutions owed foreigners even entails ceding certain claim-rights against foreign national security agents who are acting according to their professional duty. The scope of this rights-ceding is set, on the restrictive side, by the security standard, and on the permissive side, by 1) what is necessary for adversary agencies to keep their people safe and 2) what intelligence actions the rights-ceder can be modelled as accepting.[7]

On the restrictive side, inhabitants of one state can object to the actions of an adversary agency that fail the security standard, for example, if the agency is employing norms and tactics that are more unreliable, disproportionate, ineffective, inefficacious and rights infringing than alternatives the agency has at its disposal. Agencies cannot be criticized for using the best technology they can afford, even if it is less sophisticated than the technology used by the inhabitants of the targeted state. They can be criticized for failing to train in state-of-the-art tradecraft that is based on open-source information and not dependent on technology. Again, the duty to support just institutions does not justify the behaviour of corrupt or incompetent adversary agents.

On the permissive side, inhabitants of one state have a duty to support the just institutions of other states, which entails ceding the claim-rights necessary to create the moral permission for adversaries to keep their clients safe. At base, this permission will cover what are essentially investigative efforts to identify security threats. These actions include *diagnostic* collection efforts designed to anticipate threats.[8] We will assume that intelligence gathering will involve *accidental* or foreseen but unintentional (i.e. *collateral*) collection on people who are not security risks to the collecting agency's state (e.g. caught in communication with the legitimate target). One cedes claim-rights against *accidental* collection, because if agencies cannot act where there is a risk of collecting or surveilling a mistakenly targeted person, they cannot act at all. It may seem odd to cede a claim-right against an accidental action since the party to which the right is ceded cannot intentionally perform an accidental action. What this ceding involves is really an acknowledgement that the agent would not be considered to have acted negligently when an agency accidentally collects on an innocent party. Civilians' duty to support just (foreign) institutions does not directly address *collateral* collection; this has to be justified via a waiver, discussed later. The ceding of rights associated with the duty to support just institutions is also not the main justification for *direct and sustained* targeting for collection because agencies should only be doing that against security threats to their states and those targets will have either waived or forfeited rights. Given what was just said about accidental collection, innocent parties are not wronged when an agency mistakenly targets them with direct collection efforts and then breaks off collection and purges the relevant data if and when the mistake is promptly understood.

Ceding certain claim-rights that enable foreign intelligence officers to engage in collective efforts that might accidentally or diagnostically collect the information of an innocent person is part of that person's duty to support just foreign institutions protecting foreigners' rights. The scope of adversary permissions can also be widened or restricted based on waivers inhabitants of particular states can be modelled as making. These waivers may also simply reiterate the minimal permissions based on the duty to support just institutions.

One waives certain claim-rights when one enters into a permissible, adversarial practice. For example, a boxer waives his right against being hit when he engages in a bout. This dynamic also applies if one's adversarial practice is mediated by an agent, as in a lawsuit. When one sues someone, one engages a lawyer to try to seize some of the defendant's property or limit her rights. One cannot begrudge the target of one's lawsuit hiring a lawyer to defend her interests in turn. The defendant might after all be in the right or the degree of her wrong-doing may be contestable. By contrast, one cedes no rights to the agent of a fully culpable wrong-doer if one hires an agent to protect one's rights and interests. A gangster may not hire a gunman to bolster his offense against the bodyguard of an innocent person whom the gangster threatened.

So a foreign state agent's actions are potentially justified indirectly, as a reciprocal entailment of a client consenting to his own agents' outward-facing actions. If the inhabitants of state A retained claim-rights against being collaterally, diagnostically or accidentally collected on, then intelligence agencies of state B could not permissibly engage in the same protective function inhabitants$_A$ have a right to demand of (their own) agencies. This is to say that inhabitants$_B$ could not have their moral right to security met to the same degree that inhabitants$_A$ have their right met.

One cannot complain if one is targeted with the same collection tactics one wants one's own agencies to use against foreigners. Since all have the right to protection by their intelligence agencies, consent-worthy intelligence gathering norms and tactics, like consent-worthy legal norms, will be those that are acceptable to all sides equally. They have to be acceptable to one as a client or a target. Agency leaders can model their clients' consent to collection practices at two junctures. First, on the permissive side of the equation, they can ask, what action does securing national security against a particular adversary demand, given the current bilateral situation? Second, on the limiting side of the equation, they can ask, what kind of reciprocal response would clients tolerate? Answers to the second question may eliminate norms and tactics suggested by answers to the first question.

Unlike diagnostic and accidental collection, collateral collection is only justified via a waiver consequent to entering into an agent-mediated adversarial practice. Imagine that a bodyguard can only defend his principal by shooting at an unjust attacker in a way that endangers an innocent bystander. The bystander has a duty to try to rescue endangered innocent people, but not at the cost of her life. We have no grounds to say she would not be wronged if she is injured in the crossfire. Put differently, the bodyguard is not permitted to fire away, with the thought

that the bystander has ceded claim-rights against being collaterally harmed. We *could* say principals have waived rights against being exposed to collateral harm if everyone had a bodyguard and bodyguards protected their principals against both unjust attackers and other bodyguards. By hiring a bodyguard, one would be entering into a quasi-adversarial, agent-mediated practice. By parity of reasoning, we can say that agency leaders can model their clients' waivers of rights against collateral collection if they also model them as endorsing their intelligence officers engaging in collection efforts that might collaterally collect on foreigners. The agents of such an agency act permissibly when they collect their innocent persons' communications as a side effect of targeting someone with whom the innocent person communicates. Agency leaders can model this consent if and so long as it is technologically impossible to only collect one half of a conversation or textual exchange.

The reflexivity of this model should encourage a conservative attitude towards intelligence collection. We must ask on behalf of the model consenter if she can consent to her state agents using tactics abroad that, via the principle of reciprocity, she must also permit foreign agents to use against her. As will be argued later, this reflexive question also applies to intelligence officers concerning the means and extent to which they are willing to be targeted or have their relatives targeted.

Just intelligence-gathering tactics

Using this reciprocal approach, the rule of thumb should be that security agencies should use the same collection tactics abroad on non-government agents that they use domestically. For example, if the security standard indicates that warrants issued by judges are necessary for a security service to intercept a particular domestic inhabitant's communications or that a domestic criminal suspect has to be warned about a right to remain silent in police interrogation, the same treatment should apply to a foreigner targeted by the security service. Let us now consider several considerations that will present caveats to that rule of thumb. These considerations will argue for an expansion of intelligence collection powers. The second half of this section will consider the rights of different intelligence targets and non-targets, which largely constrain intelligence activities.

Practical limitations on foreign agents acting abroad or the different nature of the target might suggest different tactics leading to greater infringements on the target's rights. Police may be able to conduct line-of-sight surveillance of suspects with undercover officers, whereas such intimate operations may not be feasible against certain foreign targets, particularly in harsh terrain or repressive countries. Long-distance imaging and SIGINT technology may lead to less discriminate operations than domestic operations (e.g. a satellite image can cover a huge footprint compared to what an undercover agent can see). To say this more privacy-infringing tactic is consent-worthy under the security standard is to say the model consenter permits her adversary's security agencies to attempt the same in her country.[9] While this reciprocity is hard to imagine in some asymmetrical contexts – al-Qaeda operators shelter in the Federally Administered Tribal Area

(FATA), but anti-Pakistan government irregulars do not train in Vermont – there are plenty of peer state rivalries in which reciprocal scenarios are more likely.

A further disanalogy between foreign intelligence operations and domestic law enforcement presents an additional complication. By their nature, intelligence operations are prophylactic, dealing with prospective threats. An intelligence agency might not be adequately vigilant if it only gathered intelligence on known intelligence targets. To anticipate threats or discover new leads, intelligence agencies might wish to engage in bulk data interception and use automated searches to scan the content of the messages or scan the metadata for suspicious patterns or contacts between new numbers and known intelligence targets. Yet this kind of prospective action violates due process in that the target's privacy is infringed prior to evidence of wrong-doing. This form of collection can be made more sensitive to the targets' rights by automating the collection process so that a human analyst only reads or listens to an intercept if there is a high likelihood of its intelligence value, but this is still a significant departure from the standard balance of power between liberal state and citizen. We will need to consider if the security risks for inhabitants of one state are sufficiently grave that they can be modelled by agency leaders as endorsing the risk of being reciprocally targeted by adversary states' dragnet intelligence operations (more in the following).

A third qualification is that reciprocity is necessarily with respect to intelligence function rather than the technological expression of that function. An endorsement of intelligence agency_A's diagnostic collection including broad satellite coverage, selector-guided data intercepts and bulk data collection would permit adversary agency_B's similar diagnostic measures. Yet a wide range of concrete practices could be justified if the security standard permits security services to conduct foreign operations employing the most reliable, efficient, rights-respecting etc. tactics available to the service within a given function area. The best locally available tactics justified by the security service will vary depending on a given political entity's wealth, size, technological prowess and ingenuity. If the standard then effectively permits all security actors to "do their best", the standard allows situations in which, for example, wealthy country A's intelligence services can conduct very discriminate, sophisticated, targeted and automated intercepts of foreign intelligence target's communications – so that very few innocent people have their privacy infringed or violated – while also permitting poor country B's intelligence services to conduct relatively crude, indiscriminate intercepts that infringe on the privacy of far more innocent people. For example, the 2006 film *The Lives of Others* depicts 1980s era Stasi agents steaming open random East German citizens' letters in order to see if they contained any subversive content. This method of intercept is obviously far more invasive than an automated system that only saves communications with specific selectors for human analysis. So the leaders of technologically sophisticated agency_A, considering targeted intercepts of foreign expats_B on A's soil, would need to consider if their relatively backward adversary in state B will reciprocally respond by steaming open the mail or listening to all the phone conversations of expats_A in state B. Thus, intelligence collection activities fail the security standard in particular instances if one state's adversary's best

methods of intelligence collection are so crude as to be imagined to be intolerable to the inhabitants of the target state. In this case, intelligence officers would need to refrain from collecting from a certain state if they could anticipate that the state would retaliate by engaging in its crude collection methods (political entities with more sophisticated adversaries would not encounter this problem). That said, it is difficult to think of an example of SIGINT that would be so rights-infringing as to be intolerable for any state to suffer at the hands of its dangerous adversary if that was the price of garnering signals intelligence. One's tolerance of risk is influenced by the nature of the harm the risky activity forestalls. Crude forms of SIGINT might be intolerable if the reward for the risk was lower, such as if the target state did not pose a military threat to the collector state.

One might wonder if any states enjoy a unilateral right to collect against adversaries because of the illegitimate nature of the target government. As mentioned earlier, one can hire a bodyguard if threatened by a gangster, but the gangster does not have a right to hire extra gunmen in response. Since the security standard is indexed to the protection of negative liberty, it justifies traditional policing and national security actions of even some illiberal and/or autocratic states. While the security standard does not justify repressive actions aimed at a government's non-violent political or ideological opponents, it does justify the bread-and-butter responsibilities of a state aimed at protecting its inhabitants from street crime, piracy, terrorism and foreign military attack. I will follow John Rawls's usage referring to states that do this as well as provide internal law and order in a mostly egalitarian manner as "decent states" (I will refer to states, but it could also be the case that a political entity within an internationally recognized state might have significant autonomy and protect its inhabitants from external threats). Hence, Russia, China and Iran, for example, have the right to engage in foreign intelligence operations as a means of defending their people against foreign military attack and intelligence collection. The security actions autocratic states may legitimately engage in to protect their people also protect the autocratic regimes, which, in other moments, may repress their own people. Internal repression has to reach a high level to remove hypothetical consent to a state's national security operations. Under these conditions, foreign invasion would be rationally preferable to the perseverance of the repressive regime. The security standard does not justify the coercive actions of states with governments that largely neglect ordinary inhabitants and use power largely to benefit a ruling clique. Such governments are virtually indistinguishable from criminal gangs. I will refer to these as unjust states.

The security standard prefers the most rights-respecting out of the most practically efficacious tactics and norms that are locally feasible. We therefore have to consider the scope of intelligence targets' rights, applying the justifications for intelligence operations to specific categories of targets. In order to accomplish this aim, we have to consider both the target and the context for collection. Any SIGINT or IMAGINT operation will involve three major relevant variables: the collecting agency, the target and the agency with defensive jurisdiction over the target. Significantly, there are agencies with roughly equal technological abilities

with their adversaries; agencies with greater abilities than their adversaries and those with lesser abilities. There may also be situations where a target is in a failed or unjust state and has no intelligence agency acting on his behalf. In all the cases where a functioning and responsible agency exists, the collecting agency has to consider if the defending agency's retaliation or reciprocal actions are tolerable for the collecting agency's own citizens given the overall threat environment. This concern will likely be readily addressed in the affirmative if the collecting agency is technologically or operationally inferior to its adversary since there is a good likelihood that the adversary's relatively discriminate reciprocal response will be tolerable to the collecting agency's citizens (obviously, this would not be the case if both agencies were operating on a very crude level and one was only slightly more sophisticated than its rival). The situation facing inhabitants of failed and unjust states will be addressed at the end of this section.

I would suggest there are seven relevant categories of intelligence targets:

1 a positively identified foreign intelligence officer or service member
2 a suspected foreign intelligence or military agent (the latter might be non-uniformed)
3 a non-specific target, for example a random person collected against in dragnet fashion
4 a civilian of intelligence value, for example a politician, bureaucrat, engineer or scientist
5 the relative, lover, colleague or friend of 1–4
6 a positively identified unprivileged irregular, for example a member of a terrorist group
7 a suspected unprivileged irregular

People have rights to privacy which presumptively cover professional communications. Certainly, it is wrong for professors, doctors, accountants, priests etc. to hack each other's professional correspondence. Adversary military, privileged irregular combatant or intelligence personnel in decent states have a right to communicate their operational plans with colleagues since (according to the traditional post-Westphalian just war tradition) these professionals do nothing legally or morally wrong in pursuing national security goals. Yet since their adversaries have the same right to pursue the national security goals of their own political entities, those adversaries can engage in strategic behaviour such as intercepting their enemy's communications.[10] National security actors waive their rights against having their operational communications intercepted when they join their organizations since they know the parameters of the profession include communication interceptions. Further, assuming that the operationally significant information collected regards state secrets, foreign security personnel do not suffer personal privacy violations when their communications are intercepted. The professional secrets are in a sense, state property, like military materiel. Waiving claim-rights against being targeted with collection efforts is not the same thing as waiving rights to the information, in which case it would be wrong for the agent

to attempt to conceal the information. Intelligence officers can take steps to safeguard their communications and resist intrusions. Waiving claim-rights against being targeted with collection efforts does not entail a requirement to volunteer the relevant information any more than waiving a claim-right against being struck in a boxing match means a boxer must refrain from ducking.

Intelligence agencies will often want to collect personal information about their state agent target. The recruitment of intelligence assets from within military and intelligence agencies sometimes occurs when recruiting agents identify vulnerabilities or dissatisfactions on the part of their targets. Further, many intelligence officers work undercover. One way to identify undercover agents is to closely monitor their communications and examine the documents associated with their "legends". Certainly, intelligence officers know how their game is played, so voluntary entrance into the profession, where they are trained about information security and the professional perils of personal foibles, can be understood as amounting to a waiving of a claim-right against having their personal information being targeted by adversary collectors.

There is a greater separation between public and private for service personnel than for intelligence officers. Going to work for service personnel may mean physically deploying to a different country or to sea. Stateside service personnel conduct most of their professional work on bases in uniform using unique military materiél and using specially secured communication and data storage devices. So there is usually a physical and social separation between professional and personal lives. Unlike civilian intelligence officers, service members can readily do their jobs in most cases without intercepting their adversaries' private communications or information. Further, in most cases, their job is overt; unlike many intelligence officers, they present themselves as service personnel while working. So the personal communication and data storage of service personnel per se are usually irrelevant to adversaries; it does not relate to national security and does not identify a service member's true profession. Yet service members' personal information can be turned into a vulnerability through their own indiscretions. Damaging information is of interest to adversary agencies as it can make service personnel vulnerable to recruitment.

I do not think that it is permissible as a matter of course for adversaries to target all the private communications of service personnel and hack all their personal data files looking for leverage. Militaries need to recruit relatively large number of people. Enlistees know of course that they will be physically vulnerable to enemies in the event of war (which statistically, they may well avoid during their time of service). Since intelligence collection is prophylactic, agencies would want to collect potential blackmail material against service personnel from potential future adversaries as soon as they enter the military. It seems unrealistic to think that many potential enlistees would be willing to enlist if they knew that all potential adversaries would be invading their privacy as a matter of course and that unlike intelligence officers, they would not have the advantage of clandestine identities to shield them from adversaries' attention. So, unlike intelligence officers, who know how intelligence operations work and who have some protection in their

clandestine identities, it does not seem reasonable to think enlistees waive a right to all their personal information to foreign adversaries. Leaders of intelligence agencies would also have to consider the effect on military recruitment if this kind of information collection became the new normal, brought about in part through their universal collection of their adversary military's personal information.

Finally, like intelligence officers, privileged irregular militants engaging in guerrilla tactics typically hide in plain sight by presenting themselves as ordinary civilians when not engaged in operations. Since they dress as, and live among, non-combatant civilians, they cannot begrudge their conventional adversaries engaging in counter-insurgency to collect personal information and intercept communications on suspected targets in order to distinguish irregulars from non-combatants.

In 3) and 7) a variety of intelligence collection operations, including counter-insurgent operations, regularly produce false-positives, interdicting innocent people mistaken for militants. A clearly concerning case is where the communications of innocent people might be collected and analysed when their out of context remarks trigger automated collection or where intelligence operations wrongly indicate that a particular person is a foreign intelligence officer, intelligence asset or an irregular militant. In a domestic law enforcement context, rights-infringing investigations of suspects (who turn out to be innocent) can sometimes be justified. State agents tasked with investigative functions cannot only interact with guilty persons or people of intelligence value. Agents' mandate instead is to investigate suspects, people who might be innocent or might be guilty. Agents would not be meeting their protective duty if treating all suspects with the benign indifference they do apparently innocent people. Similarly, intelligence operations ill-serve the state if they are restricted to investigating known threats, to the exclusion of anticipating future threats. Investigations require some rights infringements like questioning, arrest, interrogation and searches. People in a just state, where state agents can be held accountable for bad behaviour, do not have their rights violated by security standard-compliant investigative actions since they can be modelled as consenting to security standard compliant norms and tactics aimed at protecting their rights. The case is more complicated in international settings since the intelligence collector is not necessarily acting to secure the community of which the target is a part and the target likely will not have the ability to identify or sue the intelligence agents who wrong her.

As an expression of their duty to support just institutions, inhabitants of one state cede claim-rights against having some of their information collected diagnostically by an adversary agency in order to ascertain if they are a security threat. This diagnostic level of collection would seem to be the minimal requirement of a duty to support just foreign security institutions. All people have a right to demand that their security agents identify looming threats. Ceding a right against diagnostic collection is a way to support this right enjoyed by foreigners. So, intelligence agencies may be justified – contingent on meeting the practical elements of the security standard – in conducting automated dragnet signal interception of civilian communications guided by selectors, in which all data from a particular

region is digitally scanned for certain security sensitive references prior to select communication being forwarded to a human analyst for consideration. Metadata recording and retention may also be justified for the same reason. Agencies might want to retain years' worth of big data in order to have a library to scan if current investigations highlight an old communication as being of significance. Agency leaders might model inhabitants of their states accepting the risk that their adversaries will store their old communications but never view them – unless the adversary finds evidence that a citizen is actually a spy or a terrorist – as a cost of their own agencies doing the same thing in a fraught security environment. Inhabitants of states without major security concerns could not be modelled as accepting this risk. The cost to civilians is steeper, and potentially less tolerable, if an adversary had very sloppy selection algorithms and so fed a large number of false-positive communications to human analysts. Still, even this cost is perhaps tolerable since the foreign analyst presumably reads an anonymized text or email. By contrast, the cost might be unbearable if the adversary's diagnostic efforts involved reading every written communication or listening to every conversation as a matter of course. Businesses might fear intercepted and stored communications more than individuals. Even if an agency is reasonably sure its rival does not engage in industrial espionage, it has to consider if domestic business actions would be harmed because of executives' fears that sensitive communications *could* be intercepted and misused or leaked.

A further point for agency leaders to consider on the subject of big data collection might relate more to the retention, rather than the collection, of the data. The cost to average citizens and businesses is greatly increased if intelligence agencies store their intercepted data on relatively insecure servers and then hackers steal the data and make it available in a searchable database. One might not worry much if one's online searches and texts are stored on an NSA or MSS server in some desert, never to be read unless one starts corresponding with jihadists, but worry very much if that information is available on a website prospective employers, spouses and divorce attorneys can search for a modest fee.

Due process protections can help make domestic criminal investigations security standard-compliant. People can demand to be protected from criminals and have crimes against them promptly solved, but innocent people also do not want to be regularly inconvenienced or frightened by ham-handed investigations and so would endorse checks on investigators by neutral arbiters to help ensure that investigations are warranted. Appealing to the reciprocal element of the security standard, inhabitants of one state would endorse due process style protections appropriate for domestic undercover work for foreign intelligence targets if their agencies needed to move beyond the diagnostic phase to target a particular person the initial diagnosis suggested was a threat. Graduated due process protections are important since the same standards inhabitants$_A$ could be modelled as endorsing could guide collection efforts targeting them on behalf of inhabitants. Some due process protections involved in an overt domestic investigation such as those involving arrest and interrogation are not apt since the target will not initially, if ever, know he is an intelligence target. The key relevant protection is

the requirement of a warrant from a neutral court prior to engaging in collection against foreign civilian targets. Collectors would have to produce evidence that the desired target is a person of intelligence value. The court should view foreign intelligence targets as having the same privacy rights as domestic inhabitants, be it with respect to their physical person, their possessions, their communications or their data. This requirement would extend to targets who are suspected of being civilian intelligence officers operating outside security-sensitive areas like intelligence agency headquarters and embassies.

Intelligence agencies might also take an interest in politicians, diplomats and civilians working in sensitive industries. Their work product on their computers and work-related communications are fair game for interception if they pose a potential threat to other states. These professionals can be modelled as waiving claim-rights against having work-related communications and devices targeted (posing a risk of collaterally capturing personal communication) since they voluntarily took jobs where they pose indirect threats to adversaries or are part of a state's overall foreign policy establishment. Security training likely regularly reminds them of what is at stake in their communications. Moreover, they should choose to be scrupulous in separating personal from professional communication.

The harder question is whether they have ceded claim-rights to all their personal data. Intelligence agencies might very much want to gather embarrassing or incriminatory information against a politician, diplomat, or defence contractor in order to blackmail him or find out personal information about him in order to improve a recruiting officer's ability to develop rapport. I suggested earlier that the security standard would likely not permit targeting service personnel in this manner because the reciprocal cost is too high. Cost is relative, so it would be more accurate to say that the cost of inviting universal collection against one's own military usually outweighs the benefit of collecting against random service personnel. The benefit of collecting damaging information against select politicians, diplomats or weapons scientists is far greater. Further, the number of people targeted is relatively small. Politicians and diplomats can be trained about the risks of extracurricular indiscretions and provided with relatively secure devices. Politicians in democracies are also partially vetted during campaigns as their opponents try to identify and publicize any damaging information. In many cases, scandals foreign intelligence agencies might discover have already been revealed to voters.

Scientists and other researchers working very closely on weapons or intelligence gathering technology can perhaps be modelled as waiving claim-rights against having personal information targeted since they likely know or should know the tactics of adversary agencies and the importance those agencies place on the scientists' work. It seems a heavy cost to researchers working on more peripheral research, perhaps on defence or intelligence grants, if their funding comes with a risk that all their personal information will be potentially collected and exploited by foreign intelligence agencies. Here, leaders of agencies would have to think very carefully if the security environment warrants reciprocal invasions of domestic researchers' privacy.

Intentionally intercepting the communication or records of friends, relatives and lovers of all the aforementioned categories is fraught. To be clear, this tactic involves separate targeting of a target's familiars, not incidentally collecting against them in the course of intercepting the target's communications. Intelligence agencies may seek personal information that could be used to blackmail targets regarding their relatives' foibles or to reveal vulnerabilities or proclivities that intelligence officers might otherwise exploit in order to cultivate the person as a spy. Intelligence officers might also offer incentives to targets to help relatives in distress.

First, relatives of service members, intelligence officers, weapons researchers etc. have not waived rights in the role-based manner of their relatives. Have they forfeited their rights by being complicit in their relative's actions? One cannot help what career one's child, parent or sibling chooses, but what about a spouse? The spouse of a service member knows about his or her spouse's profession, but an intelligence officer might never reveal his true profession to his spouse or at least not until after they are married. Bearing in mind that reciprocal element of the security standard, it seems too high a bar to demand divorce as the price of avoiding being targeted for intelligence collection. Still appealing to this reciprocal element, intelligence officers have to consider if they are willing to have their own relatives targeted for intelligence collection prior to targeting their potential assets' relatives. Such targeting violates the targets' rights. Except perhaps in the most perilous security environments, it seems the reciprocal element would preclude targeting relatives.

Finally, an international criminal like a drug dealer, a pirate or an unprivileged irregular combatant,[11] whose operational communications are intercepted, does not have his moral rights violated wherever he is located because he lacks a right to contribute to criminal operations via those communications. However, since his identity is likely not overt, the collecting agency has to go through due process steps of getting a warrant prior to targeting him. Failure to do so would violate the target's rights even if he really was a criminal.

The foregoing argument assumes that targets live in decent states with functioning governments engaging in national security work on behalf of their inhabitants. Unprivileged irregulars and other types of criminals sheltering in failed or unjust states have no more of a right to secret operational communications than they do if they are operating in just states. Service personnel and intelligence officers serving unjust regimes are effectively serving criminal organizations and so, like ordinary criminals, forfeit a right to their operational communications. Defence contractors or weapon scientists in unjust states may be closer to criminals if they are knowingly colluding with an unjust regime. Those who are coerced by their repressive governments are wronged by being targeted for collection since they have not forfeited their rights through culpable collaboration. Agencies in other states need to appeal to the doctrine of double effect or lesser evil arguments in order to justify wronging these groups of people.

Service personnel, intelligence officers and defence contractors presumably are not present in failed states. People in failed or unjust states have a duty to support

just foreign institutions as a way of respecting foreigners' rights. This duty means ceding claim-rights against diagnostic and accidental collection, but not collateral collection. Collateral collection occurs when an agent foresees that collecting against a target will also capture information from a target's interlocutors even though they are not intelligence targets. My view is that minimal diagnostic collection meant to ascertain if one is a security threat is included in the duty to support just foreign institutions, but collateral collection is only justified via a waiver consequent to entering into an agent-mediated adversarial practice. A waiver of rights against collateral collection is entailed by a modelled endorsement of one's agents engaging in collection efforts collaterally collecting on foreigners. Agency leaders can model this consent if or so long as it is technologically impossible to only collect against one member of a conversation. Thus, this justification does not extend to non-targets in failed or unjust states because these people lack intelligence agents working on their behalf against foreign adversaries.

One might think that non-targets living in unjust states have a duty to help protect foreigners from the non-targets' unjust leaders. Yet non-complicit civilians in unjust states are like hostages, victims of their own leaders and potentially threatened by adversaries as well. Their duties cannot extend beyond those of non-targets living in just or decent states. They are wronged by collateral collection. Agencies would have to appeal to the doctrine of double effect or make a lesser evil argument to justify violating these people's rights.

Collateral collection *is* permissible if it will ultimately contribute to rudimentary law enforcement benefiting non-targets like the interdiction of terrorists or drug dealers in a failed or unjust state. In that case, innocent people in the target area can be modelled as ceding claim-rights to any agency that will act in the interest of their rights when local criminals are removed from the scene.

Notes

1 Gendron, Pfaff, Diderichsen and Vrist Ronn make the same point in rejecting direct application of just war theory to intelligence operations (Gendron 2005, 418; Pfaff 2006, 75; Diderichsen and Rønn 2017, 482).

2 Pfaff and Tiel also use a social contract framework (Pfaff and Tiel 2004, 4).

3 For example, an egalitarian norm will exclude certain tactics that focus only on certain ethnic groups.

4 I make an argument for this position in Chapter 7 of my *The Moral Status of Combatants: A New Theory*.

5 The latter can be effectuated by voluntarily entering into a practice involving certain well-known concessions on the parts of members. For example, one tacitly consents to abide by the rules of a game when one voluntarily begins playing, even if those rules might force one to suffer some harm or loss. When one loses a hand in poker, one cannot object that "I wasn't playing *that* sort of poker".

6 Though, for example, one ought not to subvert foreign elections by posting disinformation on the internet.

7 Pfaff and Tiel have similar ideas, but express their ideas in a terse manner that prompts many questions.

8 Pfaff and Tiel base the permission to engage in diagnostic collection on tacit consent. Their position is vulnerable to standard critiques of John Locke's famous account of political obligation based on tacit consent. Namely, one can ask how tacit consent obtains if citizens are never provided with the express terms of the "contract" and do not have meaningful refusal options.

9 The adversary agency's permission does not mean agencies in the target state are not permitted to oppose their actions.

10 See *An Ethics of Interrogation*, Chapter 7.

11 An irregular combatant is a combatant who uses guerrilla tactics and/or represents a non-state group (often then using guerrilla tactics). An unprivileged irregular is one who fails the criteria for moral and lawful belligerency: obeying a unified chain of command, carrying one's arms in the open, wearing identifying emblems, and obeying the laws and customs of war.

References

Diderichsen, Adam, and Kira Vrist Rønn. 2017. "Intelligence by Consent: On the Inadequacy of Just War Theory as a Framework for Intelligence Ethics". *Intelligence and National Security* 32 (4): 479–93. https://doi.org/10.1080/02684527.2016.1270622.

Gendron, Angela. 2005. "Just War, Just Intelligence: An Ethical Framework for Foreign Espionage". *International Journal of Intelligence and CounterIntelligence* 18 (3): 398–434. https://doi.org/10.1080/08850600590945399.

Omand, David, and Mark Phythian. 2018. *Principled Spying: The Ethics of Secret Intelligence*. Illustrated edition. Washington, DC: Georgetown University Press.

Pfaff, Tony. 2006. "Bungee Jumping off the Moral Highground". In *Ethics of Spying: A Reader for the Intelligence Professional*, edited by Jan Goldman, 66–103. Lanham, MD: Scarecrow Press.

Pfaff, Tony, and Jeffrey R. Tiel. 2004. "The Ethics of Espionage". *Journal of Military Ethics* 3 (1): 1–15. https://doi.org/10.1080/15027570310004447.

Skerker, Michael. 2016. "Moral Implications of Data-Mining, Key-Word Searches, and Targeted Electronic Surveillance". In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley J. Strawser, 251–75. New York: Oxford University Press. www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190221072.001.0001/acprof-9780190221072.

———. 2019. "A Two Level Account of Executive Authority". In *Sovereignty and the New Executive Authority*, edited by Claire Finkelstein and Michael Skerker. New York, NY, USA: Oxford University Press.

———. 2020a. "What Can Be Asked of Interrogators?". In *Interrogation and Torture: Integrating Efficacy with Law and Morality*, edited by Steven J. Barela, Mark Fallon, Gloria Gaggioli, and Jens David Ohlin, 253–78. New York: Oxford University Press.

———. 2020b. *The Moral Status of Combatants: A New Theory of Just War*. 1st edition. Abingdon, Oxon; New York: Routledge.