

A Foundation for Government Secrecy

Michael Skerker

[Read only draft. Draft 1, Oct. 22, 2013. Readers, note: I anticipate incorporating more research on the literature on government secrecy in subsequent drafts.]

Law must be revealed to those who are expected to comply with its demands. Law is a mere pretext for coercion if the laws permitting the government to coerce people for non-compliance are concealed. So inhabitants of a state need to know what behavior their state expects of them. The purpose of this essay is to determine whether inhabitants of a liberal state—a type of state tracing the legitimacy of its coercive actions to the consent of the governed—also need to know the internal protocols and legal findings of the government agencies ostensibly serving them. To put this question another way, what, if anything, may government agencies in liberal states keep secret?

This essay will proceed in four parts. It is first necessary, in Part One, to articulate a moral foundation for security operations—law enforcement, military, and intelligence operations—conducted by a state domestically and internationally. The argument for grouping these types of operations together is that they are all oriented to maintaining a secure and peaceful domestic society. Moreover, liberal states divvy up security responsibilities among different agencies in various ways, so it would not serve the purpose of this essay to restrict the conversation to one agency or activity. A moral foundation will express the rationale for security services such as law enforcement, military, and intelligence agencies to engage in operations. This foundation will also provide a possible justification for maintaining secrecy if secrecy is necessary for the success of security operations. Part Two will ask if public scrutiny of security services is necessary. Part Three will ask if laypeople are competent to scrutinize the operations of security services. After it is determined that public scrutiny is both appropriate and possible, Part Four will consider whether and how security services can effectively

deliver peace and security while also making internal protocols, legal rulings, and operations public. I conclude that many types of security operations can survive public disclosure at a certain level of generality. A relatively small number of morally permissible operations must be kept secret when their disclosure would directly or indirectly endanger security personnel or the success of operations.

I

The proper portfolio of a liberal state can be modeled by considering the hypothetical consent of its inhabitants to potential government policies. A signal feature of the liberal state is deference to the natural autonomy of human beings. Moral respect for autonomy leads to the privileging of individuals' consent to action affecting them. This, as a way of ensuring that potentially rights-infringing behavior is consistent with the relevant persons' wills. While consent can easily be garnered on an interpersonal level, such as between business partners, it is notoriously difficult to explain exactly how citizens or inhabitants transfer their consent to government officials. There are few opportunities for unambiguous explicit consent to government policies, and even the best candidates, like oaths of citizenship or votes in referenda prompt questions about the scope of consent and implications of being in the voting minority.¹ Further, a policy's being popular, does not make it

¹ The best (i.e. least ambiguous) candidates for expressing consent are ones which rarely occur. Signing a new Constitution, swearing an oath to one, or voting for one in a referendum are suggested as paradigmatic instances of consent to a government invoked in the classic notion of the social contract (John Locke, *Second Treatise of Government* § 89; Thomas Hobbes, *Leviathan*, ch. 17; Michael Walzer, *Obligations*, (Cambridge, MA: Harvard University press, 1982), xi). The obvious difficulty is that such events have not often occurred in recorded history (David Hume, "Of the Original Contract," in *Moral and Political Philosophy*, ed. Henry Aiken, (New York: Hafner Press, 1948), 356-372, 362), and probably none have occurred with unanimous consent—a criterion the early contract theorists demanded. (A. John Simmons, *Moral Principle and Political Obligation* (Princeton: University Press, 1979), 72). Further, it is not clear how being bound to one's ancestors' oaths or votes is consonant with the autonomy the doctrine of consent is meant to safeguard (Hume, 360). Immigrating and taking oaths of citizenship or naturalization would seem to express explicit consent (Harry Beran, "In Defense of the Consent Theory of Political Obligation and Authority," *Ethics* 87.3 (1977), 260-271, 262; C.W. Cassinelli, "The 'Consent' of the Governed," *The Western Political Quarterly* 12, no. 2 (June 1959), 399; Walzer, xi), but most inhabitants of a country are born there and never participate in such events (Cassinelli, 398; *A Theory of Justice* (Cambridge, MA: Belknap, 1971), 13; M.B.E. Smith, *Is There a Prima Facie Obligation to Obey the Law?* 82 *Yale Law Journal* (1972-1973): 950-976, 960). Ritualistic performances like swearing allegiance encounter difficulties of motivation, vagueness, and scope. Compulsory performance of such rituals cannot express genuine consent. If swearing allegiance is not compulsory, what sort of political obligation accrues to non-swearers? If the performance is voluntary, the ritualistic nature of the performance militates against the likelihood that participants grasp the contractual import of their mantras. Further, is one swearing allegiance to a particular leader, a system, or a particular canon of laws? If allegiance is sworn to the third item, this further argues against the prospect that consent is knowing, given the size and complexity of a canon of laws (Cassinelli, p. 402).

morally upright, as minorities in the Jim Crow era can attest.² [fn] Tacit consent—a putative non-explicit type of consent conveyed by the willing enjoyment of government services—strikes some as a contradiction in terms and others as being too broad.³ Surely, one does not consent to every law and foreign policy initiative of a country one visits by simply driving on its roads—even if, as a matter of fact, local police can force one to comply.

The form of consent I will use in this essay is called hypothetical consent.⁴ Some object that like tacit consent, hypothetical consent really is not consent at all.⁵ True, hypothetical consent is a term of art in that it abstracts from actual acts of consent to anticipated acts of consent; to logical conditions consistent with the act of consenting; or to the logical conditions for consent. With any model of hypothetical consent, politically legitimate government actions are those that are consent-worthy by inhabitants of the state. Politically legitimate actions are proper uses of the coercive power of government, which sanctioned by hypothetical consent, do not violate the rights of citizens or inhabitants. By contrast, tacit consent is supposedly conferred on whatever laws are empirically in

² Mark E. Kann, “The Dialectic of Consent Theory,” *The Journal of Politics* 40 (1978), 386-408, 395.

³ Simmons, 80-93; Johnson, 22; Smith, 961. Also, several authors point out that while it may be technically possible to leave a nation the policies of which one abjures, emigration is a daunting, if not practically impossible task for many. (Hume, 363; Jeremy Waldron, “Theoretical Foundations of Liberalism,” *The Philosophical Quarterly* 37, no. 147 (Apr., 1987), 138; Karen Johnson, “Political Obligation and the Voluntary Association Model of the State,” *Ethics* 86 (1975), 17-29, 18-20.) These unhappy dissidents are like slaves, born into a nation that demands obedience and rejects the legitimacy of dissent with reference to an imaginary act the performance of which the dissident cannot avoid so long as he is alive. Further, if bare residency constitutes tacit consent, and that form of consent is the requirement for political legitimacy, then the criterion is empty, because all governments are legitimate. (Rawls objects to this invidious reading of Locke, 112.) If mere usage of roads constitutes tacit consent to the government, tourists and refugees would seem to be in the unhappy position of owing taxes and military service to the nation of their passage. (Johnson, 25; Walzer, 101.)

⁴ For examples, see Kant, “On the Proverb: That May be True in Theory...,” *Perpetual Peace and Other Essays*, ed. Ted Humphrey (Indianapolis: Hackett, 1983), 61-92, 79; Rawls, 11; Waldron, “Theoretical,” 138; “Special Ties and Natural Duties,” *Philosophy & Public Affairs* 22, no. 1 (winter 1993), 25. For Kant, hypothetical consent is the standard of justice for public law. For Rawls, the hypothetical consent of the representatives in the Original Position delineates natural duties and obligations. For Waldron, hypothetical consent can be what obligates inhabitants to a dominant political regime.

⁵ See Cynthia Stark, “Hypothetical Consent and Justification,” *The Journal of Philosophy* 97.6 (2000), 313-334, n. 4 for bibliography of thinkers making what she calls the “standard indictment.” Stark is right to point out that a critique denying hypothetical consent’s linkage to political obligation does not fully meet Rawls’s maneuver in that Rawls is clear he is invoking consent hypothetically—describing the nature of institutions to which fully rational choosers *would* consent, under ideal conditions—and so means to circumvent the problems of the tyrannous majority and anarchism associated with explicit consent. He *knows* actual citizens might prefer not to receive some government benefit, and so, with Locke and Tussman, Joseph Tussman, *Obligations and the Body Politic* (Oxford: Oxford University Press, 1960), is really describing a certain feature of just government when averring to consent and consent theory rather than linking political obligation to explicit consent, or in the form of tacit consent, a functionally identical stand-in for explicit consent, 332.

force when the tacit consenter is present in the state. A further theoretical component of hypothetical models is an articulation of the abstract consenter as having a particular moral make up—a precondition for determining the kind of policies the consenter would endorse in the abstract. Inhabitants, rather than citizens of states, are the relevant consenters because the hypothetical consent is modeled in reference to abstract conceptions of the human person rather than in reference to people of particular nationalities. The practical impetus and outcome of considering mere occupancy in a particular state is to justify law enforcement and legal protection of resident aliens and foreign visitors. The difficulties with actually garnering explicit consent and the puzzles involved with tacit consent are removed with a focus on hypothetical consent. Conscientious legislators and bureaucrats should endorse policies an abstract inhabitant of the state would consent to, if given the chance.⁶

Different conceptions of the moral person will create different abstract grounds for deeming actions consent-worthy. For example, if one conceived of all human beings as innately musical and only flourishing with exposure to music, legislators might reasonably judge state-funded public concerts and free universal music education to be consent-worthy. Elsewhere, I articulate a detailed moral model of the inhabitant of a liberal state for the purpose of employing hypothetical consent, but will not reproduce it here.⁷ In the interests of brevity, it probably suffices here to be intentionally vague in articulating a moral model. Since our interest here is only to justify the actions of security services, we do not need such a robust model of the human person as would be necessary to justify public education, government-funded healthcare, arts programming, or the like. The benefit of this vagueness in formulation is to develop a foundation for the ethics of security operations inclusive of many different models of autonomy and capable of incorporation into many different kinds of liberal states. To be clear, the minimal model of autonomy is not presented as a full account but as a common base insertable in more complex articulations of autonomy.

⁶ A broader explanation of why we should focus on consent models at all is more than I can do in this space.

⁷ *An Ethics of Interrogation* (Chicago: University of Chicago Press, 2010), ch. 2.

We can proceed with a minimal model of autonomy since securing certain kinds of negative rights of inhabitants (freedom from interference to rights expression) is the sort of thing security services can perform and generally are expected to perform. We can specify the aspects of autonomy relevant to security services in a very simple way. First, this innate capacity to make decisions and act is violated by violent attack, lengthy restriction of physical liberty and association, and destruction or confiscation of private property—or significant threats of these violations. Second, since it is not even coherent to speak of autonomy outside of a community of autonomous people (if rights, as an expression of autonomy, are seen as limitations on others' activities), we will also assume that a stable community, relatively free of major rights violations or the threats thereof, is a necessary background for an individual's autonomy over time. More specifically, this background is a necessary material precondition for a group of people to enjoy the full expression of their rights consistent with equal enjoyment over time. Thus, arguments about protecting autonomy will also have to take into account protection of an environment hospitable to individual autonomy. All together then, our ideal inhabitant would be modeled as consenting to government actions meant to create an environment relatively free of rights violations and associated threats.

Since government measures taken to protect against rights violations usually include types of coercion, there is a risk that measures aimed at protecting innocent inhabitants from rights violations will also actually violate those persons' rights. It therefore will not suffice simply to postulate that all protective actions by security services are consent-worthy. Without delving into specific tactics yet, we can further specify formal criteria for hypothetical consent. Any rational consentor would prefer reliable, efficacious, proportional, efficient security tactics to tactics aimed at the same result that are relatively unreliable, inefficacious, disproportionate, and inefficient. Since security-oriented tactics ranking favorably in these four categories, involving patrol, surveillance, regulation of goods and movement, arrest, use of force, interrogation, and detention, will inevitably infringe on people's rights,

our model consentor would consent to the most rights-respecting among the most reliable, efficacious, proportional, and efficient tactics. Finally, this concern for the rights of those whom security services aim to protect dictate hypothetical consent to an environment *relatively* free of rights violations.

Securing an environment completely free of rights violations perpetrated by inhabitants against one another would likely necessitate profound infringements and violations on the part of state agents.

Thus, we can proceed with a simple, admittedly broad, formal framework for judging various security-securing tactics. This moral framework will be referred to as the “security standard.” The most rights-respecting among the most reliable, efficacious, proportional, and efficient locally-available tactics aimed at securing an environment relatively free of rights violations or the threat thereof are consent-worthy, and so, politically legitimate for state agents in liberal states to employ. State agents should use the security standard in assessing which tactics to use. They should also constantly seek tactics and technologies that are more reliable, efficacious, rights-respecting, etc. Security services should be held to a realistic local standard. A military with the funding and wherewithal to use precision guided munitions should use them in order to minimize civilian casualties. A less wealthy, less technically-advanced military should not be faulted for failing to use them when aerial bombardment is otherwise the tactic best meeting the security standard. Legislators should hew to this standard when crafting laws meant to reform security agencies. The internal counsel for such agencies should interpret the letter of existing laws according to the spirit of the security standard. The public has a duty to use this standard to oversee the protocols of security services (discussed next section). Tactics falling short of this standard can be reasonably criticized and targeted for reform.

The security standard is inward-looking to the extent that it is oriented in the first order⁸ toward facilitating a community hospitable to the autonomy of inhabitants we imagine as potential consent-givers. When modeling the hypothetical consent of a generic autonomous person, we stipulate her

⁸ Hypothetical consent can also be used to seek peace and security internationally, but I will not pursue that argument here.

consent to certain actions protecting her from rights violations. In addition to protecting her and facilitating her rights exercise, this consent limits the behavior of the protected person in two ways. First, in the name of consistent treatment of all autonomous people included in the modeling group (autonomy presupposes community), we have to stipulate *dissent* to actions violating the rights of other people in that group. Such behavior violates a rule of reciprocity inconsistent with the theory's assumption of moral equality amongst abstract consenters. It also contributes to an environment that is non-conducive to autonomy. Second, in the event she does not respect others' rights, the consenter has to be understood to consent to coercive restraint of rights violations she attempts against others. For example, one hypothetically consents to being restrained from assaulting a neighbor by police such that a policeman's physically stopping the assault and handcuffing the assailant does not violate the assailant's moral rights.

The security standard also applies to tactics aimed at external threats handled by a state's military and intelligence services. Since our model consenter is merely an autonomous person, as opposed to a person of a particular nationality, the modeling group assumed for the purposes of modeling hypothetical consent is all autonomous people.⁹ This means we have to consider the effects of the consenter's choices on all other autonomous people in the world. We can assume that any autonomous person would consent to domestic government actions aimed at securing a domestic environment relatively free of rights violations. These actions include actions by military and intelligence operators aimed at defeating external threats to a state's security. There are two types of action, broadly speaking, of relevance to this enterprise: investigative and strategic. Investigative actions (undertaken by any sort of agency) approach targets who may be security threats in order to determine if they are in fact threats. These targets include domestic and international criminal suspects, foreigners who might have information of national security interest but who are not clearly-identified

⁹ I will not take up the question whether fetal life and all humans outside the womb including babies and the mentally impaired are autonomous.

members of foreign security agencies, and foreign civilians who may be irregular militants (e.g. insurgents, international jihadists). Strategic actions are actions taken against known adversaries such as foreign service members, intelligence officers, and clearly-identified irregular militants. Strategic actions lack the tentativeness and gradualness appropriate with investigative tactics, as they presuppose a clearly identified adversary; they are oriented to getting the best of that adversary.

Since all people in the world can be modeled as consenting to a regime of outward-facing security-seeking actions, a model consenter's consent to foreign operations by her security services also potentially justifies action by foreign agents targeting her. This dynamic can best be explained by discussing its domestic parallel. Hypothetical consent is permissive when it comes to the justification of police tactics meant to keep the model consenter safe. Considerations of how to secure the safety of a model consenter justifies a series of actions aimed at rights violators or potential rights violators. At the same time, a principle of reciprocity, justifying police behavior targeting the consenter if the consenter is suspected of perpetrating or planning rights violations, urges restraint of police tactics. So the consent that we imagine autonomous people extending to domestic security-seeking tactics takes into account that they might be the target of those tactics. The same reflexivity must apply to outward-facing security-seeking tactics. The security standard is oriented toward a pre-conventional notion of autonomy expressed in natural rights so an articulation of outward-facing tactics should begin with an assumption that foreigners will be treated the same as domestic inhabitants when the government interacts with them for the same reasons. The nature of military and intelligence operations might expand the menu of actions potentially consent-worthy beyond those countenanced in domestic situations (e.g. using more destructive weapons, more below), but as in policing contexts, this trend is limited by the principle of reciprocity, which would extend the same liberty of operations to foreign state agents.

So, regarding investigative actions, the model consenter must use herself as a reference point,

asking whether 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. Using this approach, the rule of thumb should be that security agencies should use the same investigative tactics abroad that they use domestically. For example, if the security standard indicates that warrants are necessary for a security service to intercept a 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. There might be exceptions if the foreign target is significantly different than a domestic one or if it is not feasible to extend the same treatment to foreigners as to domestic inhabitants. As examples of the former type of difference, the sophisticated encryption technology foreign intelligence officers use might prompt different monitoring tactics than appropriate for domestic criminal suspects. As an example of the latter kind of difference, certain types of up-close, manpower-intensive surveillance feasible for a domestic security agency might not be feasible in an adversary state. In this case, an intelligence agency might want to opt for satellite or drone surveillance—a tactic that might be more privacy-infringing since it permits seeing over walls shielding targets from street-level surveillance. If this more privacy-infringing tactic is consent-worthy under the security standard, the model consenter potentially permits her adversary's security agencies to do the same in her country.

The approach outlined here creates a universal norm for security operations. Foreign security agencies can be criticized for failing to meet the security standard when it is in their power to meet it. An example would be if an intelligence agency bugs the room of every foreign tourist, even though it is capable of targeting select foreigners of intelligence value. Regarding a similar concern, one might wonder if state agents should not adhere to local standards of security operations when operating abroad. This concern might seem particularly germane in cases when it appears expedient to treat foreign combatants or intelligence targets in a less deferential manner than domestic criminal suspects.

Yet one obviously does not want one's state agents using less reliable or less efficacious tactics abroad even if they are in a foreign state whose own security forces use less reliable and efficacious tactics. While one would want one's state agents to emulate foreign practices better than their own when operating abroad, practical limitations may make this impossible.

Regarding strategic actions, aimed at state agents, the model consenter is conceived first as being a civilian benefitee of military and intelligence agency protection. The principle of reciprocity dictates that foreigners can benefit from the same protections, so the model consenter consents to outward-facing strategic actions by her military and intelligence personnel aimed at foreign state agents, with two limitations. First, military and intelligence tactics are only consent-worthy from the perspective of a civilian if she can consent to being collaterally harmed by them when those tactics are targeted at her own state agents. Thus in a military context, tactics imposing a certain level of risk on foreign civilians are only consent-worthy if the model consenter can consent to the risk of being collaterally harmed when foreign militaries use the same tactics in operations in the consenter's homeland. So, for example, the security standard endorses the traditional tenets of *jus in bello*—just warfighting. Tactics must discriminate between military and non-military targets, and not cause more damage than is warranted by the military value of a target. If one can be modeled as consenting to other states' militaries deploying to war to defend their domestic inhabitants, even if one's own state is the unjust aggressor, one would not consent to foreign tactics pursuing this just cause in an unnecessarily destructive manner, targeting civilians or causing more civilian casualties than proportionally offset by the good of achieving tactical goals.

This modeling exercise suffices to limit military and intelligence operations insofar as they affect civilians. One would also need to model hypothetical consent from the perspective of a military or intelligence professional in order to determine the limits of military and intelligence operations insofar as they affect state agents. This follows because state agents properly direct strategic actions at

other state agents. In some cases, overlapping justifications would yield the same limitations as the civilian-based consent exercise. For example, civilians cannot be modeled as consenting to be directly targeted in military operations since such actions violate their rights and service personnel cannot be modeled as consenting to directly targeting civilians because such targeting is not a reliable nor efficient means of achieving a military victory (e.g. killing civilians instead of enemy service personnel leaves the enemy's military capacity intact). There would also be tactics failing the security standard that can only be modeled from a service member's perspective since only germane to him, such as tactics using chemical weapons or napalm against massed infantry. I will not pursue service personnel-based consent-modeling further here.

In all, the security standard prompts a cautious approach, particularly to foreign operations, because 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. The best locally available tactics justified by the security service will vary depending on a given state'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 conduct very discriminate, sophisticated, targeted, and automated intercepts of foreign intelligence target's communications—so that very few innocent people have their privacy violated—while also permitting poor country B's intelligence services to conduct relatively crude, indiscriminate intercepts that violate the privacy of far more innocent people. So too in the case of war: the military of wealthy country A may cause far less collateral damage with precision munitions than the military of country B, despite the fact that B's military is trying just as hard to be discriminate and proportional.

II.

i.

Having articulated a moral standard for judging the operations of security operations, it is next important to consider the form oversight should take. Is it enough for security operators to self-regulate or for their agencies to self-regulate through the actions of internal auditors like staff lawyers and inspectors general? Or must the public conduct oversight of these operations, or at least of the internal protocols and legal findings setting the parameters for operations?

It first important to clarify the practical dynamics of oversight. It is a less pressing matter to assign and specify a duty of oversight as a distinct activity in cases of explicit consent when consent immediately precedes the contracted activity, like the purchasing of an item at a store. It is also less pressing when consent is tacitly given throughout the duration of the relevant activity,¹⁰ since consent can be revoked at any time (by explicitly objecting), such as in the provision of a service involving the client's participation or active enjoyment like a medical procedure, massage, or haircut, or in some consensual activity like game-play, debate, sex, etc. In these cases, oversight of the service provider's or activity partner's activities by a concrete, particular consenter is simultaneous or nearly simultaneous with consent to the activity. By contrast, hypothetical consent only creates abstract standards; compliance with standards has to be conducted empirically. Then, concrete, particular individuals can and should offer their explicit consent to consent-worthy activities or explicitly dissent to activity failing this standard. So, from a practical perspective, government transparency is important since there is usually a lag between the execution of a governmental action and the effect on an inhabitant or foreigner or a significant number of people unaffected by government actions targeted at others. These gaps inhibit real-time oversight concurrent with on-going tacit consent. People need to know what state agents are doing in order to assess post hoc whether the agents are hewing to the security standard legitimating their behavior.

¹⁰ This is a legitimate invocation of tacit consent since the boundaries of the putatively consensual activity are definite and clear to the putative consenter and of such a routine nature that it can be assumed that the putative consenter understands the consequences of the action.

It is important to clarify here that I mean people need to know about their state agents' actions in a practical, and not normative, sense of “need.” Political legitimacy comes from consent-worthiness in my theory, not actual consent and not openness to publicity. The reasons actual consent is not the desired standard has already been discussed. Let us now to turn to the openness to publicity standard. This standard of political legitimacy would reject any policy that could not be revealed without destroying its efficacy. Many contemporary exponents of the standard look to Immanuel Kant’s signal articulation of the idea in *To Perpetual Peace*. Kant argues that “all actions that affect the rights of other men are wrong if their maxim is not consistent with publicity.”¹¹ He means that an action is immoral if the general rule guiding the action cannot be known by all without that widespread knowledge making the execution of the action impossible. Impossibility of execution would accrue because the action's success inherently depends on the maxim remaining covert in the way that a lie's success depends on its remaining covert or because it would necessarily create universal opposition in the manner of a person's announcement of his policy of murdering anyone he dislikes. David Luban convincingly argues that Kant's “publicity principle” does not preclude all forms of secrecy. True, “first-order secrets” cannot be revealed without frustrating the action or identity the secret is meant to conceal, e.g. “John Smith is actually an undercover officer.” However, “second-order secrets”—secrets about secrets—can be revealed without destroying the relevant first-order secret. “The police department utilizes undercover officers” can be publicly disclosed without identifying any particular undercover officers and so passes Kant's publicity standard: it is not self-frustrating and would not necessarily create opposition.¹² The possible disclosure of the second-order secret makes concealing the related first order secret permissible. These kinds of second-order secrets about general government policies are relevant to our topic, so we need to ask if the publicity principle would preclude the

¹¹ Immanuel Kant, “To Perpetual Peace,” appendix II, [381] 135, ed. Humphrey.

¹² David Luban, “the Publicity Principle,” *The Theory of Institutional Design*, ed. Robert E. Goodin, (Cambridge: Cambridge University Press,), 154-198, 191.

concealment of second-order government secrets.¹³ In this event, government spokespeople would not reveal that it utilizes undercover officers and presumably would either refuse comment or lie if asked about the general tactic.

The publicity principle is an implied element of Kant's central moral principle, the Categorical Imperative. There are at least three ways the publicity principle can be understood when applied to liberal democratic states. I will use the term "openness to publicity" to express this application in order to emphasize the abstract consenters' relation to it. The broader publicity principle embedded in the Categorical Imperative captures an aspect of the possible universalization morally sound maxims display: they can still be efficacious even if universally known. Universal knowledge of the maxim is a pre-condition for its permissibility. By comparison, the relevant aspect of positive law is that it is assessable to inhabitants, i.e. they could actually go to a library or the internet and read the statute. An attendant feature of permissible positive law is that the law would not necessarily create opposition once it was studied.

The view that any plan or policy depending on secrecy is inherently tawdry—morally wrong independent of its political use—must be rejected. Such a view would condemn such innocuous actions as planning a surprise birthday party or hiding an anniversary gift. The next two views are consistent with the policy not being inherently immoral. The morally problematic aspect of the second view relates to the moral grounds for government coercion in liberal political theory. Policies need to be *open* to oversight in order to meet the conditions for citizens' consent (they do not actually need to meet with their consent, for the reasons already articulated). Concealed policies are not even candidates for political legitimacy because of an absence of the conditions necessary for citizen endorsement of the actions—even if the law would have been popular.¹⁴ By way of analogy, a man wrongs a woman if he

¹³ Pozen refers to the concealment of second-order secrets, "deep secrets" and regards them with deep distaste because the public does not even know to ask about them, David E. Pozen, "Deep Secrecy," 62 *Stanford Law Review* 257 (2010), 274.

¹⁴ Pozen sympathetically outlines this view, 286.

has intercourse with her while she is too drunk to give informed consent, even if she would have given her consent if sober. A third reading of the openness to publicity standard is a practical one: opacity to oversight creates an opening for corruption, even if the policy is itself sound.

I do not find the second reading of the openness to publicity standard compelling in all cases because I can think of (and will discuss below) intuitively permissible security-seeking tactics which lose their efficacy if the *fact* of their use is revealed. These are second-order secrets that need to remain secret in order to be effective. Such acts of concealment do not pass the second view of the openness to publicity standard. The difficulty for that standard is that the concealed tactics, along with their protection, still seem legitimate; indeed, the security standard can justify their use. This claim about seemingly legitimate concealment of second order secrets does not itself fully defend the security standard as the criterion for political legitimacy, but explains why I prefer it to the openness to publicity standard. Thus, for the sake of argument, for the moment, we will entertain the possibility that the existence of some government programs are legitimately kept secret. However, since no program (inclusive of the program staff) is self-monitoring, proper guidance of these programs can only be promoted with external oversight of some sort. Thus, I will proceed below, taking the third, practical view of the openness to publicity standard as the relevant one. On that view, external oversight or the possibility of external oversight is not constitutive of a program's legitimacy, but important in order to ensure that legitimate programs do not become corrupt. Section Three will address the obvious tension between the need to oversee a program which cannot persist if its existence is publicly revealed.

ii.

We can now expand on the idea that government programs practically need external oversight in order to ensure compliance with their moral authorizations. Again, government programs are not self-monitoring and do not win real-time tacit or explicit consent from state inhabitants in the manner of a massage. The public has interests, rights, and duties relevant to oversight of government security

services which would be trespassed if state agents err, overreach, or become corrupt. First, an inhabitant has an interest in ensuring that his own rights are not being violated by the government. One is obviously in a privileged, though still fallible, position to judge whether one is being wrong by another. Some might also term this interest a duty, though duties to the self—such as a duty not to be made servile—are less widely-recognized than duties to others. This duty to the self can be supported by an associated duty to others in the following way. It is likely that the government will perform the same rights-violating actions against others if one does not protest the government violating one's own rights. Thus, allowing the bad behavior to continue unchecked fails to protect others.

One has a right to oversee government activities for the reason that a contracting party has a right to see the work he has purchased. A taxpayer has a right to see the services he subsidized with his tax monies. The purpose of this type of oversight of government actions is to combat fraud and waste.

Regarding duties, inhabitants of liberal states alienate certain powers to state agents to use on their behalf. Principals are morally responsible for their agents' behavior when that behavior is consistent with the principals' orders so the principal has a duty to ensure that her agent is doing things she is morally required to see accomplished and not doing things she herself is morally forbidden to do.¹⁵ This applies both to direct agents, who do relatively low-skilled actions the principal could have done herself like gardening, babysitting, and proof-reading, and to free agents, highly-skilled actors like lawyers or accountants the principal relies on for their expertise and ability to make independent judgments.¹⁶ Obviously, the moral impetus for the public to oversee state agents is greater than the impetus to oversee private agents because of the potential harm these free agents can do utilizing the

¹⁵ A principal is not responsible for something her agent did completely of his, the agent's, own accord, having nothing to do with the agency transferred to him by the principal.

¹⁶ Free agents bear a heavier burden of independent moral responsibility than direct agents for electing tactics the principal does not have the training to fully understand. Practically, principals can usually not exercise real-time oversight of free agents because of a lack of relevant expertise and so will likely focus on consequences, which are intelligible to a layperson in a way tactics are not. Oversight will then likely be expressed in reform efforts rather than proactive guidance. For example, the average civilian, supportive of a given military operation, does not have the expertise to decide what weapon systems should be used in a particular attack, but can demand to know if some more discriminate tactics or technology is available after a large number of civilian casualties are incurred in an operation.

powers of the state.

There are two specific duties the public has to meet when overseeing state agents. First, contributing to an environment relatively free of rights violations or the threat of rights violations is a subsidiary positive duty of the negative duty to respect others' autonomy since this rights-friendly environment is a material pre-condition for individual autonomy.¹⁷ Therefore, inhabitants of a state have a positive duty to their fellow human beings residing in the state to ensure that state agents are indeed working to secure an environment relatively free of rights violations.¹⁸ Second, since the coercive means state agents use to prevent rights violations perpetrated by state inhabitants against each other can themselves violate people's rights, the public must ensure that its agents are pursuing the end of security in ways conforming to the security standard. In other words, the public has a duty to ensure that its agents pursue the moral end of security (creating an environment relatively free of rights violations) without violating deontological concerns making state security morally valuable.

Since the behavior of state agents abroad can incur responses from foreign state agents, it is in the public's self-interest and consistent with their concern for their neighbors to oversee their agents' behavior and object to unnecessarily provocative or otherwise immoral behavior abroad. Assuming that behavior abroad potentially creates a reasonable foundation for in kind foreign responses, the public should object to practices that exceed the security standard marking what they would tolerate being done to themselves. This limitation has to be considered in kind rather than degree, given that a certain kind of operation releases the adversary government from engaging in the same kind even if they can only perform it in a cruder fashion than the first government. Thus, for example, the public should object to their security agencies intercepting foreign civilians' private communications electronically if they are unwilling to countenance less-sophisticated foreign agencies doing the same to them by

¹⁷ This might sound strange, but another example of a negative duty creating a subsidiary positive duty would be the duty not to harm others leading to a positive duty to ensure one's car is in good working order, one's gun is securely locked, and one's pool is fenced.

¹⁸ Other relevant positive duties include paying taxes and complying with all but egregiously unjust laws of any state one lives in or visits.

steaming open envelopes.

III.

The public has a duty to oversee state agents, yet may not be competent to execute this duty. Usually, duties imply the duty-bound person's power to perform the duty but this is not always the case. For example, one may find it hard to observe the duty not to unjustly harm others when operating a new vehicle or tool and learning too late that it is difficult to control.

In many cases, the general public is not competent to technically assess the internal protocols of security agencies. One would often need as much knowledge as an expert practitioner to know if a weapon system, a computer code, or interrogation technique is the most reliable, efficacious, proportionate, efficient, and rights-respecting available. However, the general public is competent to assess whether the effects of a given tactic raise moral concerns. For example, the public does not know if stopping and frisking random young men in high crime areas is really the most efficient or reliable method of inhibiting gang violence, but does know that this tactic is disruptive to neighborhood life and offensive to innocent people accosted by police. This concern is enough to begin a conversation with state agents about whether this tactic really is the best available, and if so, whether the good done is really worth the harm.

In order to assess the actions of state agents, the public needs a good understanding of not only the actions of state agents but of the threats the agents' operations are designed to meet. For example, one cannot assess the proportionality of a response unless one understands the danger being faced. Concerns related to the public's knowledge of state agents' operations will be addressed in Section Four. The public's being informed about the threats security agencies are trying to meet creates a different problem, particularly in the international arena. In some cases, a detailed picture exposes sources and methods of intelligence gathering to the state's adversaries.¹⁹ The adversary can learn about

¹⁹ Thompson notes this possibility in Dennis Thompson, "Democratic Secrecy," 114 *Pol Sci Q.* (1999), 186.

the threat-publishing state's technological capacities like its satellite or other aerial reconnaissance resources (and flight paths), based on the imagery released, and its signal intercept (SIGINT) capacities, based on the electronic communications released. This knowledge both helps the adversary prepare to destroy or jam those assets in case of war and helps the adversary hide the strategic assets that have been shown to be vulnerable. More dangerous still, is the direct threat posed to undercover operatives or their intelligence assets who are the sources of the sensitive information describing the foreign threat. There will be sensitive programs in the adversary state's defense and intelligence apparatus known only to a few, and the process of elimination conducted by counter-intelligence agents when such programs are compromised can be brutal and swift.

So there will be times when a government would need to describe a threat in order to justify expenditures or operations at a level of specificity it cannot describe without jeopardizing sources and methods of intelligence collection. These are moments of irreducible tension between the need for oversight and the security aims civilian oversight is meant to secure. A government's concealment of a sensitive threat assessment amounts to what Luban calls a third-order secret: a secret policy justifying keeping secret a program encompassing secret operations. Luban does not think keeping third-order secrets concealed can be justified as it gives unchecked power to officials.²⁰ I recognize the risk in permitting third-order secrets, but external oversight should usually be omitted in cases where oversight meant to check compliance with the security standard threatens to contravene the goals of the security standard. By way of analogy, standardized testing of students should be curtailed if it gets in the way of their education. Again, according to my theory of political legitimacy, lack of oversight does not inherently nullify legitimacy. Lack of oversight is a practical, rather than a constitutive problem in that it creates risk of corruption. By way of analogy, if we assume getting drunk is not inherently immoral, getting drunk is still problematic because it creates the risk of various kinds of bad behavior and injury.

²⁰ Luban, 191.

The security standard justifies keeping these types of enemy-alerting threats secret; as it should, the intelligence-gathering operations meant to assess the threats, and the contingency plans developed to meet them. The expenditures on personnel and equipment designed to counter the threat should also be kept secret if their nature is so specific as to tip the hand to the adversary, e.g. if country A buys chemical-resistant suits for all its service personnel, adversary country B will realize that its secret chemical weapons program has been exposed (the dollar amount can be disclosed).

The security standard also limits this secrecy. Disclosure would undermine efforts made to secure the security of the state, jeopardizing the inhabitants of the state. Yet only those operations meeting the security standard that would be compromised by publicity should be kept secret. Still, the risk of corruption remains. Let us return to Luban's concern over unsupervised government officials participating in these putatively legitimate secret threat assessments and briefings. A third-order secret could perhaps be revealed regarding threats without self-frustrating or incurring necessary opposition to the secret if it were couched in the following manner. "The government will conceal certain threat assessments from the public, the detailing of which would reveal sources and methods of intelligence gathering—threat assessments that in turn may justify programs which also cannot be revealed without revealing sources and methods." Yet unlike the disclosure of a second-order secret like "the police department will utilize undercover officers," the disclosed third-order secret is too vague and too broad to give people anything substantive to consent or dissent to. As Luban writes, this kind of permission would give officials *carte blanche* to do anything on the international scene without any accountability. The proposal about concealing threat assessments would have to be rejected because of its vagueness, as opposed to its objectionable nature.

So, if secret threat assessments are sometimes legitimate, these are times when state agents have to operate on their own recognizance. This situation does open the door to corruption and abuse and so necessitates the careful vetting and training of recruits to security agencies. Disclosures of sensitive

threat assessments and secret operations *would* be indicated if corruption and incompetence hindered state agents from actually securing their state.²¹ An imperfect compromise designed to mitigate the tension between security and oversight would be to have an oversight body of legislators who themselves were sworn to secrecy. This option is imperfect because overseers committed to secrecy have no legal way of alerting the public or their colleagues outside of the select committee if the security services ignore their concerns and the wider legislature does not act on their necessarily vague, unclassified recommendations.²²

IV.

Section III broached the key question of this essay: what types of government actions are properly classified and kept out of public view? We now have a formal answer implied by the forgoing discussion of threat assessments. Operations, expenditures, recruitments, protocols, internal legal rulings, and threat assessments meeting the security standard but which cannot be revealed without jeopardizing the relevant operations should be classified. This section will specify the programs meeting this criterion. A surprising number of military and intelligence operations can be revealed to the public, at least at a certain level of generality, without harm to national security. In order to make substantive recommendations about what sort of secrets should be classified, I will consider five typical activities of intelligence agencies and three typical activities of the military. Analysis of concrete activities will produce five stock rationales arguing for or against secrecy.

SIGINT - The key question to consider when judging security operations is whether disclosure of government actions will directly or indirectly endanger state agents or civilians and whether disclosure will lead adversaries to cease activities from which the government is currently garnering useful intelligence. Cyber espionage is consistent with public disclosure at a certain level of generality

²¹ This argument creates a standard for whistle-blowing. Revealing threat assessments or programs whose efficacy depends on secrecy is not appropriate, but revealing gross abuses by state agents in the prosecution of these programs may be appropriate, provided one meets some criteria similar to those appropriate for civil disobedience.

²² Pozen makes a similar point, 332.

(i.e. second-order revelations). It can be revealed that state agents attempt to collect classified information from adversaries' computer networks and even that a particular foreign agency is targeted. This follows, because, in the digital age, every technologically-sophisticated state assumes its adversaries are attempting cyber espionage and every such state is engaged in cyber defenses including encryption, information assurance activities, and intrusion and malware detection (call this assumption that the adversary is already engaged in defensive operations the Defense argument). First-order disclosures that would compromise a specific operation should remain secret, e.g. “agents posing as defense contractors plan to use zip drives infected with the XYZ virus to install a back door in the Quds Force network this July.”

Secrecy is appropriate with respect to more traditional SIGINT, the collection of communications via the interception of various kinds of microwave and other electromagnetic transmissions. Disclosure of a state's ability to capture certain kinds of transmissions will can lead to their enemy halting usage of that technology, such as al Qaeda's alleged halting of satellite phone communications after the media revealed that US agencies could monitor the calls and also use their signatures for targeting purposes in 1998 (call the adversary's abandonment of tactics in reaction to its enemy's abilities the Avoidance argument).²³ This is a key example of a program that I believe passes (or could pass)²⁴ the security standard but the existence²⁴ of which must be concealed lest the purpose of the security standard not be met. Revelation of the second-order secret makes the program inefficacious. This is the case even if the adversary has no choice but to use the form of communication in question, because they will presumably communicate less than they would have otherwise. The need for secrecy is mitigated to a degree if the intercept capability is understood to be less than comprehensive such that the adversary can wager that there is a reasonable chance that his

²³ Whether the leak directly led to al-Qaeda's change in procedure is contested. Cf. “Bush Account of a Leak's Impact has Support,” David E. Rosenbaum, nytimes.com, publ. Dec. 20, 2005 and “File the Bin Laden Phone Leak Under ‘Urban Myths,’” Glenn Kessler, washingtonpost.com, publ. Dec., 22, 2005.

²⁴ As noted in section Three, a civilian has a limited ability to assess whether a given operation has better available tactical alternatives.

communication will slip through the collector's net (call this the Randomness argument). Once it is widely known that an agency can collect a certain kind of communication signal, secrecy is still appropriate regarding operations collecting transmissions from particular targets. Al-Qaeda closed down a communication channel after it was leaked that NSA monitoring had led to an intercepted order from Aymin al-Zawahiri to Al-Qaeda in the Arabian Peninsula leader Nasser al-Wuhayshi to attack US embassies in the Middle East.²⁵ It should also be noted that while SIGINT raises privacy concerns, the elimination of SIGINT as an intelligence source forces agencies to rely more on human intelligence (HUMINT). HUMINT is far more fraught than SIGINT in that it involves the penetration of undercover agents into enemy territory, the corruption of foreign intelligence assets, the enabling and financial support of criminals, and the interrogation of detainees.

HUMINT - “Turning” intelligence assets, that is, convincing members of adversary states with access to security-sensitive information to reveal the information, is the most traditional occupation of intelligence officers. Secrecy about HUMINT operations is unnecessary on a general level because of the Defense and Randomness arguments. Publicly revealing that undercover intelligence officers from state A are attempting to turn assets in state B tells state B nothing it did not already assume and was not already attempting to root out with its own counter-intelligence operations. Secrecy should be maintained with respect to specific operations along the lines of “the Agricultural minister from country A—who's really an intelligence officer—is attempting to turn Gen. X in the Strategic Air Command.” Obviously, both the undercover agent and the prospective intelligence asset are endangered by disclosure. Assuming that the undercover agent is conducting a just mission, his life is of moral value apart from the inherent value of all people; his being compromised puts his state at greater risk (this is the case even if he fails in his mission but is able to escape safely) (call this the Danger argument).

Covert Operations – Paramilitary operations conducted by undercover (i.e. non-uniformed)

²⁵ “Qaeda Plot Leak Has Undermined U.S. Intelligence” Eric Schmidt and Michael Schmidt, newyorktimes.com, Sept 29, 2013.

operators including assassination, incitement, and sabotage bear some similarities to HUMINT operations. General disclosure that agents may conduct covert operations in an adversary state is permissible because of the Defense and Randomness arguments. Specific disclosures are forbidden because of the Danger and Avoidance arguments. The Danger argument would apply in all cases while the Avoidance argument would be particularly apt in the case of sabotage, such as when state A ensures that the rare components for some weapon system or computer network procured by the adversary security services are defective or contain listening devices or malware. The adversary would know not to install the components if the plan was disclosed.

Interrogation- There is an argument to keep interrogation tactics secret because adversary agents may be able to prepare for them, thus reducing their effectiveness. This argument is more germane for non-coercive stratagems than coercive tactics (which do not pass the security standard anyway). It would be useful for security agents or irregular militants to know that interrogators of their adversary typically engage in certain kinds of emotional manipulation, for example, playing on detainees' fears, sense of loyalty, resentments, etc., or that interrogators offer fake incentives, e.g. promises to assist detainees' family members or to forgo sentences in exchange for information. However, the Defense and Randomness arguments suggest that disclosure is not overly problematic. Knowing that adversary interrogators might play on detainees' concern for their families or comrades does not eliminate the fact that detainees will be concerned for their families and comrades. Given that emotional backdrop, even the savvy detainee who is dubious of the interrogator's attempts at rapprochement might seize on the possibility that *this* interrogator is telling the truth about helping family members or minimizing the suffering of comrades.

Cryptography- The fact that a security agency tries to break its adversary's codes can be revealed because of the Defense and Randomness arguments. The Defense argument can justify disclosure of attempts to break the encryption of particular networks so long as the adversary already

knows that other states is aware of the network. For example, disclosure that agency A is attempting to break the codes protecting the computer networks of its adversary's nuclear facilities is permissible but not if the adversary thinks its nuclear program is still clandestine. As with SIGINT, specificity may lead to the adversary closing down networks protected by insecure encryption.

The following three subjects pertain to the military.

Battleplans – Standing contingency plans can be disclosed at the level of generality where they would be obvious to potential adversaries, e.g. a Russian tank invasion of the Fulda Gap will be met with NATO armor and air assets (the precise number of assets used should remain classified). There is also little incentive to keep secret even less obvious plans from weaker adversaries who do not lack the resources to respond to the battleplans. For example, there is no reason to keep secret, contingency plans to attack an adversary with stealth bombers if neither the enemy state nor its allies have any way of detecting these bombers (call this the Asymmetry argument). Otherwise, specific battle plans for imminent operations must be kept secret because of the Danger argument.

In certain cases, foreign aggression can be deterred through an adversary's ambiguous plans for response. Chinese officials might suspect that the US will not really go to war to defend Taiwan, but the possibility that the US would may be sufficient to deter aggressive moves to restore Taiwan to mainland control. Non-interventionist plans should be kept secret in cases where deliberate ambiguity serves as a deterrent to hostilities. In a similar case, plans to omit reciprocal responses should be classified if deterrence is maintained by the adversary's logical assumption that a certain action would earn a reciprocal response. For example, British ballistic missile submarines are said to have handwritten notes from the Prime Minister with orders of what the captain should do if Britain is attacked with nuclear weapons. It is appropriate to keep these instructions classified since adversaries' reasonable assumption that British submarines would retaliate in case of nuclear attack serves to deter a

rational adversary.²⁶

Deterrence maintained by false, explicitly announced policies is a harder case. For example, in the run up to the Gulf War, the Bush administration supposedly made it known to Saddam Hussein through diplomatic channels that a chemical attack on Coalition forces would be met with an American nuclear strike. I suspect this was a false threat. There are obvious moral concerns involved with a government lying to its own people if a false threat is made more publicly. There is a considerable literature on this subject raising some of the above-mentioned issues regarding government secrecy which I will not address here except to touch on a point relevant to the security standard. There is less impetus to disclose the truth about a covert false threat if the ultimate rationale for government transparency is to reform policies inconsistent with the security standard. This, because the actual policy is not inconsistent with the security standard. Whether or not the policy of making false threats to adversaries is consistent with the security standard depends on its prudence. While lying to an adversary may initially seem less problematic than lying to a domestic audience, false threats may increase tensions and make the adversary more aggressive and more entrepreneurial with its intelligence operations. Yet one can also imagine cases where lies are prudent instances of deterrence.

Troop movements – In cases of active hostilities, troop movements have to be kept secret because of the Danger argument.

Location of military assets – During peacetime, the location of strategic assets designed to deter a peer adversary, such as cold war-era American and British ICBMs, has to be kept secret on account of the Defense argument. This argument also applies to any military assets in active theaters of war. The location of assets designed to deter or to respond to weaker adversaries often do not need to be classified because of the Asymmetry argument. For example, the drone operators stationed at Creech Air Force base in Nevada, engaged against operations against the Taliban in Afghanistan do not need to

²⁶ Luban makes a similar point, 164.

fear an enemy lacking any expeditionary capabilities.

Conclusion

In liberal states, security services should seek to secure an environment relatively free of rights violations to inhabitants through the most reliable, efficacious, efficient, proportionate and rights-respecting tactics available. This standard undergirds just coercive actions by state agents and should guide internal reviews of policies and interpretation of relevant law. The public has a duty to oversee the activities of government security agencies in reference to the security standard. Nonetheless, the security standard takes precedent over oversight in cases when disclosure would neutralize the efficacy of security-seeking tactics. Secrecy is indicated for government policies meeting the security standard when revelation of these policies would directly endanger state agents or indirectly jeopardize national security by drying up intelligence sources. These areas of secrecy open up opportunities for corruption and abuse, risks that can partly be mitigated by oversight from a select group of citizens (legislators, judges, perhaps even ordinary citizens who have security clearances). These select committees are imperfect solutions to the basic tension between security and secrecy because their inability to disclose their privileged information limits their ability to end immoral or wasteful programs when they are in the minority of their committees or when the security services ignore the committees' objections. I believe this tension is an irreducible risk attendant to liberal societies, akin to the possibility of intolerant religions flourishing under a government guaranteeing freedom of religion or illiberal parties coming to power in a democratic process. The solution to the security dilemma, as in the other inherent difficulties of liberal systems, is the cultivation of the virtues of citizens and public servants.