ARTICLE

Intelligence Communities, Peer Constraints, and the Law

Ashley Deeks[*]

[*] Associate Professor, University of Virginia Law School. Thanks to Bill Banks, Jen Daskal, Zachary Goldman, Kristen Eichensehr, Aziz Huq, Rebecca Ingber, John Harrison, Richard Morgan, Paul Stephan, Pierre Verdier, Ben Wittes, and participants in the NYU Center for Law & Security Intelligence Oversight project and a University of Chicago International Law workshop. Thanks also to several current and former U.S. and foreign officials who provided helpful reactions to the ideas contained herein.

Abstract

Widespread disclosures about Western intelligence activities have shone a harsh spotlight on intelligence oversight. Many now doubt that the best-known overseers—legislatures and courts—can provide effective oversight to constrain and modulate intelligence collection and covert action. Yet the extent to which intelligence communities are and can be constrained is a critical question in today's debates about counter-terrorism and the privacy-security balance.

This article identifies and analyzes for the first time another important, law-driven source of constraint on intelligence services: their peers. Through various mechanisms—formal and informal, public and private—one state's intelligence service affects how another intelligence service conducts interrogation, detention, and surveillance; the amount and type of intelligence the other service receives; and, less tangibly, the way in which the other service views its own legal obligations. These constraints complement the more public, transparent, and expected sources of oversight and offer unique benefits that include a granular understanding of operations and an ability to minimize the politicization that frequently accompanies intelligence critiques.

Conventional wisdom suggests that interactions among intelligence services allow each actor to engage in legally prohibited actions with impunity and without accountability. This article tilts the prism to argue that, in some circumstances, these relationships impose peer constraints that result in increased individual rights protections. Peer constraints are likely to become more prevalent as intelligence services face more statutory and judicial regulation, more leaks, and more litigation. As a result, it is critical to understand when, where, and how these constraints can and do operate. This article seeks to initiate and inform that conversation.

Table of Contents

Introduction

Recent widespread disclosures about certain intelligence activities by several Western governments have prompted heated public debate about the legality, morality, and political wisdom of those activities. But the debate also has focused on the role and efficacy of intelligence oversight in constraining and modulating intelligence activities more generally. The best-known sources of intelligence community oversight are entities prescribed in statute: parliamentary committees, inspectors general, and courts. In recent years, the media and non-governmental organizations have demonstrated that they, too, can play a watchdog role over intelligence activities, even if they lack formal authority to review, alter, or sanction those activities.[1] Executive branch lawyers themselves enforce political and legal constraints on intelligence activities.[2] Yet even this range and quantity of oversight has often proven insufficient and unsatisfying.

This article identifies and analyzes for the first time a different, law-driven source of constraint on a given intelligence community (IC): its peer ICs.[3] Peer ICs are the intelligence services of foreign states with which a state's intelligence community works, whether on a one-off operation or in a decades-long partnership. One IC can impose forms of discipline or structural limits on the activities of its counterparts, particularly when it implements its own domestic and international legal obligations.[4] Through various mechanisms—both formal and informal, public and private—one state's IC can affect the way in which another IC conducts activities such as interrogation, detention, targeted killings, and surveillance; the amount and type of intelligence the other IC receives; and, less tangibly, the way in which the other IC views its own legal obligations.[5]

---

[1] *See generally* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 (2012) (arguing that the Executive faces a wide number of constraints on its actions, for reasons that include widespread internet access, leaks of classified information, and aggressive litigation by ACLU). Other actors such as the International Committee of the Red Cross can play an oversight role when intelligence agencies conduct detentions during armed conflict.

[2] GOLDSMITH, *supra* note 1, at xi–xii.

[3] I use the concept of "peer ICs" to include the ICs of states that work together cooperatively on a long-term basis across different areas (including political, military, and economic spheres) and may be parties to collective self-defense treaties, such as NATO, as well as ICs that cooperate with each other on discrete issues. The partnership between the United States and United Kingdom is an example of the first type. The discrete cooperation between the United States and Iran to identify possible members of Al-Qaeda immediately after September 11, 2001 is an example of the second type. *See Iran Gave U.S. Help on Al Qaeda After 9/11*, CBS NEWS (Oct. 7, 2008), http://www.cbsnews.com/news/iran-gave-us-help-on-al-qaeda-after-9-11/.

[4] One scholar has argued that ICs may constrain each other based "almost exclusively (on) shared professional ethos rather than law." Elizabeth Sepper, *Democracy, Human Rights, and Intelligence Sharing*, 46 TEX. INT'L L.J. 151, 153 (2010). I argue that law itself provides direct and indirect constraints in this context.

[5] We might think of these influences broadly as establishing "accountability": "A is accountable to B when A is obliged to inform B about A's (past or future) actions and decisions, to justify them, and to suffer (a penalty) in the case of eventual misconduct." Andreas Schedler, *Conceptualizing*

More broadly, one state's legal limitations can constrain joint operations. It is unsurprising that an IC is constrained by laws enacted by its own legislature. What is surprising is that the nature of IC relationships can lead to second-order effects that result in one state IC being constrained not only by its own domestic laws and rules but also by the laws and legal interpretations of other states.

The idea of "peer constraints" is intended to capture the limitations imposed on an IC in excess of those imposed by the IC's own state. Measured against a baseline of an IC's domestic laws and regulations, peer constraints are those rules that, in the context of intelligence cooperation, decrease the IC's operational flexibility. Another way to view the relationship between two ICs is as a series of transactions in which one IC "pays" for the other IC's cooperation. That "payment" sometimes takes the form of legal restrictions, which the first IC must accept if it wishes to complete the transaction. Even in the face of peer constraints, the first IC may be in a better overall position than if it were unable to obtain any cooperation from its peer. Nevertheless, the first IC is more fettered than it would be if it could conduct the operation alone, something that is increasingly rare. For this reason, the article terms these effects "peer constraints."

These constraints complement the more public, transparent, and expected sources of oversight,[6] though they cannot replace them.[7] Indeed, peer constraints offer certain benefits that may be absent from other forms of oversight, including a granular understanding of operations, technologies, and techniques that those who are not intelligence professionals lack, and an ability to minimize the politicization that frequently accompanies public critiques of ICs. Peer constraints are likely to become more prevalent as ICs face more law, more leaks (such as those by Edward Snowden and Chelsea Manning),[8] and more litigation. As a result, it is critical to understand when and how these constraints operate. Some scholars have bemoaned the lack of oversight and accountability surrounding liaison relationships.[9] This article tilts the prism to argue that, rather than

---

Accountability, *in* THE SELF-RESTRAINING STATE: POWER AND ACCOUNTABILITY IN NEW DEMOCRACIES 17 (Andreas Schedler et al. eds., 1999).

[6] In many states, courts, inspectors general, and legislative committees play roles in overseeing the intelligence services.

[7] This article assumes an inherent value in "oversight" in the broadest sense, as a means to amplify legal compliance, minimize lawlessness, and foster a certain level of transparency, while recognizing that some forms of oversight can be ineffective or politicized. *See* Ian Leigh, *More Closely Watching the Spies: Three Decades of Experiences*, *in* WHO'S WATCHING THE SPIES?: ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY 6 (Hans Born et al eds., 2005).

[8] Thomas C. Bruneau & Kenneth R. Dombroski, *Reforming Intelligence: The Challenge of Control in New Democracies*, *in* WHO GUARDS THE GUARDIANS AND HOW: DEMOCRATIC CIVIL-MILITARY RELATIONS 145, 163 (Thomas C. Bruneau & Scott D. Tollefson eds., 2006) ("If the intelligence agencies know that in the future their files will be open for public scrutiny, they are logically more likely to keep a rein on the behavior of their members."). Declassification is one mechanism by which IC activities come to light, though many states declassify intelligence information only after long time periods. Leaks are another mechanism; they tend to reveal more recent information.

[9] Sepper, *supra* note 4, at 169–72; Richard J. Aldrich, *International Intelligence Cooperation in*

maximizing flexibility, these relationships in some cases actually impose constraints that result in increased individual rights protections and, at least among Western democracies, promote convergence around more restrictive substantive rules governing intelligence operations.

The idea that peer ICs can constrain each other will undoubtedly be met with skepticism from some corners, especially in the wake of the U.S. Senate Select Committee on Intelligence Report (SSCI Report) on the CIA's detention and interrogation program.[10] Some critics may acknowledge that peer ICs influence each other, but at the same time doubt that the influence pushes in a rights-protective direction. Others may argue that powerful states such as the United States need intelligence cooperation from their peers only on the margins, and can easily walk away from constraining peer pressure without incurring significant security costs. Still others may note that the states that are best positioned to constrain often need cooperation from those states least likely to care about human rights. It is the goal of this article to identify and explicate the ways in which peer mechanisms can and do impose real, though modest, constraints that produce more rights-protective behavior, notwithstanding those arguments.

The article proceeds in four parts. Part I sets the stage by explaining why and how peer intelligence services interact. Part II defines the concept of "peer constraints" and argues that several contemporary developments, including leaks and litigation, are making peer constraints both more robust and more important to understand. Part III identifies and analyzes several forms of peer constraints, offering a number of examples to provide texture to the account. Part IV highlights the ways in which peer constraints uniquely can influence IC activity. This part also considers and responds to potential critiques of the claim that peer constraints exist and can help protect individual rights.

I. Co-operation Among Intelligence Communities

Before exploring the ways in which IC interactions produce constraints, it is necessary to understand the contexts in which intelligence cooperation occurs. Although cooperation among ICs remains one of the most secret aspects of intelligence activity, it is possible to identify the basic reasons why state ICs cooperate, as well as how they do so.[11] This Part describes how and why ICs

---

Practice, *in* INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY 18 (Hans Born et al. eds., 2011).

[10] For general critiques of intelligence liaison relationships, see Martin Scheinin & Mathias Vermeulen, *International Law: Human Rights Law and State Responsibility*, *in* INTERNATIONAL INTELLIGENCE COOPERATION AND ACCOUNTABILITY, *supra* note 9, at 252; Sepper, *supra* note 4; Francesca Bignami, *Towards a Right to Privacy in Transnational Intelligence Networks*, 28 MICH. J. INT'L L. 663 (2007).

[11] Aldrich, *supra* note 9, at 21.

interact with each other, with a specific focus on the increase in cooperation among ICs in the past decade.[12]

A. *Why Intelligence Communities Interact*

ICs interact because they must.[13] ICs are inherently secretive, driven by the goal of providing their own country with important and accurate information to allow their policymakers to make the best decisions possible. If one IC had the capacity to obtain all of the intelligence it needed on its own—using signals intelligence, human intelligence, and other sources of information—it would not need to turn to liaison services to obtain information. Likewise, if one IC had the capacity to conduct covert operations, unfettered, worldwide, that IC would not need to work with liaison services. But that is not the state of the world.

In practice, a single IC cannot obtain on its own all the coverage it requires or desires, particularly as the sources of terrorism, transnational crime, and proliferation emanate from increasingly remote parts of the world.[14] Other services will have better linguists and more nuanced cultural understandings of geopolitics. For example, the Mossad, Israel's foreign intelligence service, is skilled at monitoring situations in the Middle East.[15] The United Kingdom has history and expertise in South Asia, such that the intelligence its foreign intelligence service gathers in Afghanistan and Pakistan is in high demand.[16] Other peer services may be able to gain access to intelligence targets more easily than some Western countries could. Still others have more nuanced understandings of local terror groups.[17] As Martin Rudner puts it, "All intelligence agencies enjoy certain comparative advantages. In some cases, these may derive from functional, tradecraft, or technical attribution—largely based on specialization expertise, knowledge resources or technological solutions. In other instances the comparative advantage of intelligence agencies may derive from

---

[12] *Id.* at 25 ("The most important change in the practice of intelligence since 1989 has been the exponential increase in complex intelligence cooperation.").

[13] For a basic discussion of the reasons that intelligence services collaborate, see ERIC ROSENBACH & AKI J. PERITZ, BELFER CENTER, CONFRONTATION OR COLLABORATION? CONGRESS AND THE INTELLIGENCE COMMUNITY 50–53 (2009). As evidence of the importance that the U.S. IC places on its foreign relationships, see Marc Ambinder, *The Real Intelligence Wars: Oversight and Access*, THE ATLANTIC, (Nov. 18, 2009) (discussing fight between CIA and DNI for control over appointing senior intelligence representatives in foreign countries).

[14] Aldrich, *supra* note 9, at 32.

[15] Marta Sparago, *The Global Intelligence Network: Issues in International Intelligence Cooperation* (2006), http://pgi.nyc/archive/vol-1-issue-1/The-Global-Intelligence-Network.pdf.

[16] Ravi Somaiya, *Drone Strike Lawsuit Raises Concerns on Intelligence Sharing*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/world/drone-strike-lawsuit-raises-concerns-on-intelligence-sharing.html.

[17] Dana Priest, *Foreign Network at Front of CIA's Terror Fight*, WASH. POST (Nov. 18, 2005) (describing "sometimes reluctant foreign intelligence services [that] had much more intimate knowledge of local terrorist groups and their supporters"), http://www.washingtonpost.com/wp-dyn/content/article/2005/11/17/AR2005111702070.html.

geography, where they enjoy a locational advantage, or from a socio-cultural affinity."[18]

Cooperating with foreign peers reduces physical risks to ICs that otherwise would be forced to operate in unfamiliar territory.[19] This cooperation also allows ICs to share the cost and workload of processing information. For example, the "Five Eyes" arrangement, which includes the United States, United Kingdom, Australia, New Zealand, and Canada, allocates electronic surveillance collection among its members. For instance, Australia is tasked with intercepting communications emanating from Asia, because it is easier as a practical matter for Australia to intercept those communications than it is for the other partners to do so. The Five Eyes arrangement also provides for an exchange of intelligence personnel; joint regulations for handling the most sensitive material; standardization of terminology and code words; and methods of and limits on distribution of shared intelligence.[20]

This IC cooperation has increased with the rise of non-state actors and globalization. Richard Aldrich argues that states have increased cooperation among their ICs because of the need to address borderless problems such as financial instability, pandemics, and networked terrorist threats by non-state actors.[21] As a result, states must cooperate with a wide group of states that may not be obvious partners.[22] For example, Iran provided intelligence to the United States in the wake of the September 11 attacks, to help the United States identify non-state actors who fled Afghanistan in the wake of that event.[23] Since September 11, the United States has relied on counterterrorism-related intelligence from states such as Tunisia, Egypt, Morocco, Jordan, and Pakistan.[24]

---

[18] Martin Rudner, *Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism*, 17 INT'L J. INTELLIGENCE AND COUNTERINTELLIGENCE 193, 216 (2004).

[19] Charles Faddis, Bin Ladin's Location Reveals Limits of Liaison Intelligence Relationships, CTC SENTINEL (SPECIAL ISSUE) 15 (May 2011).

[20] JEFFREY RICHELSON & DESMOND BALL, THE TIES THAT BIND: INTELLIGENCE COOPERATION BETWEEN THE UNITED KINGDOM/UNITED STATES OF AMERICA COUNTRIES – THE UNITED KINGDOM, THE UNITED STATES OF AMERICA, CANADA, AUSTRALIA AND NEW ZEALAND 142–44 (1985); JAMES BAMFORD, THE PUZZLE PALACE: A REPORT ON AMERICA'S MOST SECRET AGENCY 309 (1982).

[21] Aldrich, *supra* note 9, at 19; *see also id.* at 21 (describing cooperation among "improbable partners"); Bjorn Muller-Wille, *For Our Eyes Only? Shaping an Intelligence Community Within the EU*, EUR. UNION INST. FOR SEC. STUDIES, Occasional Paper No. 50, at 5 (Jan. 2004) ("Detecting and assessing the so-called 'new threats' correctly requires increased intelligence cooperation between . . . agencies from different countries.").

[22] *See, e.g.*, John Davis, *Vital Cog: African Intelligence Efforts and the War on Terrorism*, *in* TERRORISM IN AFRICA: THE EVOLVING FRONT IN THE WAR ON TERROR 225 (John Davis ed., 2010) (describing U.S. intelligence relationships with Morocco, Algeria, and Kenya).

[23] *See supra* note 3.

[24] Tom Lansford, *Multinational Intelligence Cooperation*, *in* COUNTERING TERRORISM AND INSURGENCY IN THE 21ST CENTURY: STRATEGIC AND INTERNATIONAL PERSPECTIVES 430–31 (James J.F. Forest ed., 2007).

When considering why ICs cooperate, it is important to recognize that such cooperation has its own political economy. Different ICs have stronger or weaker reputations for competence, capacity, and respect for the rule of law. Each IC must balance decisions about sharing (and, in return, receiving) intelligence against the costs of leaks that come whenever additional people gain access to information.[25] ICs also will balance the costs of revealing their sources and methods against the benefits of the cooperation they hope to achieve in exchange. States with robust capacities to collect intelligence have more to bargain with. States that are less technologically capable may have comparative advantages in terms of knowledge of local groups and languages but often lack absolute advantages over the higher-technology states. This article takes up the effects of this disparate bargaining power in Parts III and IV, when considering which states can act as constrainers and whether superpowers can be constrained.

B. *How Intelligence Communities Interact*

Cooperation among ICs takes different forms. One type of cooperation consists of full-fledged liaison relationships, where states exchange intelligence officials. A second type of cooperation involves intelligence information sharing. A third form of cooperation is intelligence operations sharing, which occurs when intelligence services work together to conduct an operation such as a covert action.[26] Within the category of intelligence information sharing, states may choose to allocate collection responsibilities among themselves; to share raw intelligence; or to share intelligence assessments.[27] The Five Eyes arrangement described *supra* is a prime example of signals intelligence information sharing. Likewise, EU member states have established the "Club of Berne," a partnership of EU states' security and intelligence services that exchanges intelligence about transnational threats.[28] Many bilateral and multilateral intelligence exchanges occur, including between and among the Five Eyes member states and other NATO countries, Japan, South Korea, and Israel.[29]

One example of intelligence operations sharing is Alliance Base. Alliance Base is a joint center in Paris staffed by the CIA and intelligence services of France, the U.K., Germany, Canada, and Australia.[30] The ICs at Alliance Base plan and undertake joint counter-terrorism operations in the field.[31] Those

---

[25] In addition, sharing intelligence creates a risk that the receiving state may misuse it; relying on intelligence from another state contains a risk that the intelligence is incorrect.

[26] Aldrich, *supra* note 9, at 22 n.13 (quoting Bradley H. Westerfield, *America and the World of Intelligence Liaison*, 11 INTEL. AND NAT'L SECURITY 523 (1996)).

[27] RICHELSON & BALL, *supra* note 20, at 135.

[28] Rudner, *supra* note 18, at 210; Press Release, "Club de Berne" meeting in Switzerland, Gov't of Switzerland (Apr. 28, 2004), http://www.ejpd.admin.ch/ejpd/en/home/aktuell/news/2004/ref_2004-04-28.html.

[29] RICHELSON & BALL, *supra* note 20, at 170.

[30] Aldrich, *supra* note 9, at 31.

[31] *Id.*; Dana Priest, *Help From France Key in Covert Operations*, WASH. POST (July 3, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/07/02/AR2005070201361.html.

operations have resulted in the detention and prosecution by France of several suspected terrorists.[32] After the September 11 attacks, the CIA reportedly also established joint operation centers in two dozen other countries, each of which serves to track and capture terrorists and disrupt Al-Qaeda's logistical and financial chains.[33] The idea behind these "counterterrorist intelligence centers" is to empower foreign ICs to help the United States combat Al-Qaeda, an approach the United States has found to be very successful.[34] More recent examples include the reported renditions of Abu Omar from Italy to Egypt (which involved operational coordination between the U.S. and Italian ICs) and of Khaled el Masri from Macedonia to Afghanistan (which involved operational coordination between the U.S. and Macedonian ICs). Similarly, Stuxnet, a computer worm introduced into computers in an Iranian nuclear facility to damage its centrifuges, reportedly was a joint operation between the United States and Israel.[35] The United States and Israel also apparently cooperated in 2008 to kill Hezbollah operative Imad Mugniyeh in Syria.[36]

These are just some of the many forms that informational and operational cooperation can take. Such interactions occur frequently among various sets of states, involve direct contacts between officials in peer ICs, and implicate the legal frameworks that regulate each intelligence service involved in that cooperation. As a result, these interactions require each intelligence service not only to understand its own domestic and international legal obligations, but also to be attuned to those of its counterparts.

II. Drivers of Peer Constraints

Peer constraints arise directly from interstate intelligence cooperation. For example, when the U.S. IC intends to act in concert with Germany's IC, provide intelligence to Germany's IC, or receive intelligence from Germany's IC, the United States must comply with its own laws. As a result, U.S. laws help shape the form in which that operation or intelligence sharing takes place. Germany's IC ends up being constrained not only by its own domestic laws and rules but also by U.S. laws and legal interpretations. Likewise, the U.S. IC is constrained by both U.S. and German laws. Peer constraints describe limitations imposed on an IC in excess of those imposed by the IC's own laws. Measured against a baseline of an IC's domestic laws and regulations, peer constraints are those rules that decrease that IC's operational flexibility.

---

[32] Priest, *supra* note 31.
[33] Priest, *supra* note 17.
[34] *Id.*
[35] Ellen Nakashima & Joby Warrick, *Stuxnet was work of U.S. and Israeli experts, officials say*, WASH. POST (June 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.
[36] Adam Goldman & Ellen Nakashima, *CIA and Mossad killed senior Hezbollah figure in car bombing*, WASH. POST (Jan. 30, 2015), https://www.washingtonpost.com/world/national-security/cia-and-mossad-killed-senior-hezbollah-figure-in-car-bombing/2015/01/30/ebb88682-968a-11e4-8005-1924ede3e54a_story.html.

Peer constraints are not new. As long as ICs have been governed by law and have felt compelled to act consistently with those strictures (as most democratic services will), those ICs have had the need—and capacity—to impose constraints on the other ICs with which they cooperate. So why give more attention or credence to peer constraints today? What drives today's increased search for mechanisms of constraint? Are there reasons to think that constraints operate more robustly today than they have in the past? This Part identifies three phenomena that, both independently and interdependently, have conditioned the overall political and legal environment in which ICs now operate. A combination of leaks about IC programs, litigation challenging those programs, and the growing body of law that applies to IC programs has set the stage for a pervasive interest in more rigorous oversight of ICs. More specifically, this combination has created a situation in which states and their ICs face increased pressures (for legal, political, or economic reasons) to constrain each other.

These developments are happening in the context of the changing nature of the security threats that many states face. When ICs primarily targeted other states in order to understand those states' foreign policies, military capabilities, and future intentions, less domestic and international law regulated that intelligence activity. Now, however, ICs have shifted their focus to non-state actors, and the way they collect electronic communications implicates the phone calls and emails of many private citizens. For many states, this means that more of their domestic and international legal obligations (such as those that regulate government interference with individual rights) potentially constrain their activities. This, in turn, increases the prevalence and power of peer constraints.[37]

A. *Leaks and Other Disclosures*

Edward Snowden's leaks of U.S. National Security Agency (NSA) information revealed significant amounts of highly classified information about U.S. and foreign electronic surveillance programs, including the breadth and depth of various government capabilities. These leaks illustrated the extent to which the United States and other states spy on the communications of each other's leaders. The leaks and other disclosures also contained information about NSA programs that collected massive amounts of telecommunications and internet metadata (and in some cases content) from average citizens, both U.S. and foreign. And although revelations about the NSA have dominated the headlines, the United States is hardly the only state that engages in clandestine data collection (often in bulk) on foreign citizens. Disclosures have come to light about bulk collection by France, Germany, Belgium, Sweden, and the U.K.[38]

---

[37] Much of the discussion below focuses on the United States but other states (particularly Western democracies) are subject to similar pressures.

[38] Adam Entous & Siobhan Gorman, *Europeans Shared Spy Data with U.S.*, WALL ST. J. (Oct. 29, 2013), http://www.wsj.com/articles/SB10001424052702304200804579165653105860502; Steve Erlanger, *France, Too, Is Sweeping Up Data, Newspaper Reveals*, N.Y. TIMES (July 4, 2013),

Though the Snowden leaks have occupied the spotlight for the past year, there have been many other disclosures in the past decade about secret or covert intelligence programs. For example, leaks from within the U.S. government revealed that President George W. Bush authorized the CIA to use lethal force against members of Al-Qaeda[39] and to undertake covert action against Iran to destabilize its government.[40] WikiLeaks released secret State Department cables revealing programs such as covert assistance to the Government of Colombia to fight the *Fuerzas Armadas Revolucionarias de Colombia* (FARC).[41] The U.S. executive branch appears to have authorized some of the revelations, as when former CIA Director Leon Panetta revealed shortly after the U.S. action in Pakistan that killed Osama bin Laden that the United States had undertaken the raid as a covert action.[42] Disclosures of this sort are relevant as state ICs consider whether and how to cooperate with each other, particularly as they have become increasingly aware that their cooperation may come to light in the future.

Further, the media, human rights groups, and other private actors have independently uncovered a number of intelligence activities that have produced tangible harm to people or objects and, by virtue of the ease of Internet communications, they have made their discoveries widely known. These intelligence operations include Stuxnet, a computer worm that destroyed about 1,000 Iranian nuclear centrifuges. Computer scientists discovered the worm when

---

http://www.nytimes.com/2013/07/05/world/europe/france-too-is-collecting-data-newspaper-reveals.html?_r=0; Gregor Peter Schmidt, *Belgian Prime Minister Angry at Claims of British Spying*, DER SPIEGEL (Sept. 20, 2013), http://www.spiegel.de/international/europe/belgian-prime-minister-angry-at-claims-of-british-spying-a-923583.html; Benjamin Wittes, *Mark Klamberg on EU Metadata Collection*, LAWFARE (Sept. 29, 2013), https://www.lawfareblog.com/mark-klamberg-eu-metadata-collection; Spencer Ackerman & James Ball, *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ*, THE GUARDIAN (U.K.) (Feb. 28, 2014), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo; Ewen MacAskill, *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, THE GUARDIAN (U.K.) (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa. *See generally* Ira Rubinstein, Greg Nojeim & Ronald Lee, CTR. FOR DEMOCRACY & TECH., *Systematic Government Access to Personal Data: A Comparative Analysis* 14 (Nov. 13, 2013); *A Transnational Perspective on Section 702 of the Foreign Intelligence Surveillance Act: Hearing before the Privacy and Civil Liberties Oversight Board* (Mar. 19, 2014) (prepared testimony of Christopher Wolf, Partner, Hogan Lovells LLP), https://www.pclob.gov/events/2014/march19.html.

[39] Tara McKelvey, *Inside the Killing Machine*, NEWSWEEK (Feb. 13, 2011), http://www.newsweek.com/inside-killing-machine-68771 (describing interview with former CIA lawyer regarding targeted killing covert action).

[40] Brian Ross & Richard Esposito, *Bush Authorizes New Covert Action Against Iran*, ABC NEWS (May 24, 2007), http://blogs.abcnews.com/theblotter/2007/05/bush_authorizes.html (describing covert action finding authorizing CIA to use propaganda, disinformation, and currency manipulation to pressure Iranian regime).

[41] Dana Priest, *Covert action in Colombia*, WASH. POST (Dec. 21, 2013), http://www.washingtonpost.com/sf/investigative/2013/12/21/covert-action-in-colombia/.

[42] CIA Chief Panetta: Obama Made 'Gutsy' Decision on Bin Laden Raid (PBS NewsHour television broadcast May 3, 2011).

it spread to computers outside of Iran.[43] Another example is the work of European parliamentarians and rights groups to track alleged CIA "rendition flights" throughout Europe.[44] Journalists and non-governmental organizations have investigated targeted killings in Yemen and Somalia—research that has undoubtedly been made easier by virtue of the fact that drone strikes, unlike, say, efforts to recruit a foreign asset, produce visible physical effects. These reports collectively highlight previously unknown aspects of intelligence activities, including their geography, scope, and targets.

By definition, these intelligence activities are not exposed to democratic debate until they come to light. Sometimes the revealed activities are relatively uncontroversial, as least as a domestic matter. Consider, for instance, President Bush's 2007 authorization for the CIA to undertake covert action to destabilize Iran's government.[45] Few U.S. citizens are likely to object if the United States puts pressure on the Iranian government using non-lethal tools. Other activities, however, have prompted far more concern, due in part to the fact that some of these IC activities directly implicate individual privacy and, occasionally, life and liberty.[46] In the face of these newly disclosed programs, members of the U.S. and foreign publics, U.S. elites, foreign leaders, corporations, and civil liberties groups have all pressured Congress and the executive branch to terminate or limit some of these government activities. States such as the United Kingdom and Australia face similar pressures.[47] Indeed, a relatively unusual alignment of interests has formed among corporations, elite opinion, and many "ordinary

---

[43] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2013), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

[44] Dick Marty, *Alleged secret detentions and unlawful inter-state transfers involving Council of Europe member states*, Report to Council of Europe Parliamentary Assembly, June 7, 2006, http://assembly.coe.int/committeedocs/2006/20060606_ejdoc162006partii-final.pdf.

[45] *See supra* note 40 (describing covert action finding authorizing CIA to pressure Iranian regime).

[46] *See* Aldrich, *supra* note 9, at 20 (describing intelligence operations today as "more kinetic and more controversial"); *id.* at 31 (describing ICs as moving beyond passive intelligence gathering to "fixing, enforcing and disruption"); The Report of the Detainee Inquiry 5.7 (Dec. 19, 2013) [hereinafter U.K. Detainee Inquiry], http://www.detaineeinquiry.org.uk/wp-content/uploads/2013/12/35100_Trafalgar-Text-accessible.pdf (reciting SIS assertion that before 2001 U.K. SIS was not experienced in interviewing detainees in the field as a result of lack of prior operational need). Compare developments in the military field. In the 25 years after Vietnam, many U.S. military engagements involved "closer-than-usual contact with civilians and raised hard law-of-war issues – especially about detention, interrogation, and rules of engagement – that lawyers were vital in sorting out." GOLDSMITH, *supra* note 1, at 127. As IC activities involve (and are understood to involve) "closer-than-usual contact with civilians," it should not be surprising that IC lawyers assume an increasingly important role in helping operators navigate the laws.

[47] Sam Ball, *UK approves mass surveillance as privacy battle continues*, FRANCE 24 (Dec. 7, 2014), http://www.france24.com/en/20141207-uk-tribunal-approves-mass-surveillance-privacy-battle-continues-gchq-snowden; Ewen MacAskill & Lenore Taylor, *Australia's spy agencies targeted Indonesian president's mobile phone*, THE GUARDIAN (U.K.) (Nov. 17, 2013), http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone.

citizens"—all of whom are pressuring states to impose greater regulations on IC activities.[48]

B. *Litigation*

Leaks and other disclosures about IC programs not only provide a wide range of actors with the means to critique ICs; they also foster litigation. The greater the number of facts—confirmed or alleged—that are known about intelligence programs, the greater the opportunity for those who oppose those programs to initiate civil litigation to halt or alter them.[49] There are two ways in which this has occurred.

First, disclosures of information about IC activities have a direct effect on the availability of litigation as an option, because the disclosures may alter courts' assessments of jurisdictional issues such as standing and privileges such as the state secrets privilege. Consider, for example, the changing analysis of standing in a series of cases challenging certain electronic surveillance allegedly conducted by the U.S. government under the Foreign Intelligence Surveillance Act (FISA).[50] In *Clapper v. Amnesty International*, decided before the Snowden leaks, the Supreme Court concluded that the plaintiffs, who claimed that NSA's surveillance was unconstitutional, lacked standing to challenge Section 702 of the FISA Amendments Act because their claims were too speculative and were based on a predicted chain of events that might never occur.[51] After the Snowden leaks, in similar cases brought by plaintiffs against the NSA and other defendants challenging the NSA's use of Section 215 of the PATRIOT Act, two federal courts have found that comparable sets of plaintiffs had standing because the NSA's collection under Section 215 covered virtually all phone calls that passed through U.S. telecommunications providers.[52] Although the programs considered

---

[48] Ashley S. Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015). The extent to which these pressures will result in meaningful changes to domestic or international laws remains to be seen.

[49] Prosecutors (and, in some states, private citizens) have initiated criminal investigations and some prosecutors have brought criminal cases against foreign intelligence officials who they believe engaged in unlawful acts. This includes prosecutions of a number of U.S. intelligence and military officials in Italy for allegedly rendering a radical sheikh from Milan to Egypt. Craig Whitlock, *Testimony Helps Detail CIA's Post-9/11 Reach*, WASH. POST (Dec. 16, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/12/15/AR2006121502044.html. The Italian court convicted those U.S. officials in absentia. A German prosecutor investigated whether NSA tapped Angela Merkel's cell phone, but has been unable to find sufficient evidence to initiate a case. Alexandra Hudson, *No proof so far that NSA bugged Merkel's phone: prosecutor*, REUTERS (Dec. 11, 2014), http://www.reuters.com/article/2014/12/11/us-germany-usa-spying-idUSKBN0JP1QG20141211.

[50] Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801–1885c (1978).

[51] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

[52] Klayman v. Obama, 957 F. Supp.2d 1, 9 (D.D.C. 2013) (holding that plaintiffs had standing to challenge NSA's bulk telephony metadata collection because their fear of being surveilled was not merely speculative); Am. Civil Liberties Union v. Clapper, 959 F. Supp.2d 724, 738 (S.D.N.Y. 2013) ("Here, there is no dispute the Government collected telephony metadata related to the

by the Supreme Court and the lower federal courts are distinct, it seems likely that the lower courts would have followed the Supreme Court's standing analysis in *Clapper* to dispose of the cases before them, but for the Snowden disclosures.[53] The Second Circuit ultimately held on the merits that Section 215 did not authorize the type of collection the U.S. government had undertaken.[54]

Leaks have another implication as well. In the past decade, as intelligence operations have come to light, many plaintiffs in U.S. and European courts have challenged the legality of different forms of IC activity on the merits. This creates a contemporary role for courts that stands in contrast to the highly cabined role they historically have played in overseeing ICs.[55] In the United States, an individual who had been subject to rendition sued a CIA contractor, alleging that the company flew rendition flights on the CIA's behalf.[56] In another instance, the father of a U.S. citizen whom the United States placed on a secret, lethal targeting list sued the United States, seeking a judicial declaration that his son could only be killed in a limited set of circumstances.[57] In the United Kingdom, a former Guantanamo detainee challenged the legality of U.K. intelligence activities, claiming the United Kingdom provided information to the United States with which the latter questioned him using harsh interrogation techniques.[58] In another case, a son of a man allegedly killed by a U.S. drone in Pakistan sued the United Kingdom's Government Communications Headquarters (GCHQ), claiming that GCHQ employees had abetted murder by providing locational intelligence to the CIA so that it could target the man.[59] Another U.K. court recently allowed an

---

ACLU's telephone calls. Thus, the standing requirement is satisfied."), *aff'd in part, vacated in part, and remanded*, 785 F.3d 787 (2d Cir. 2015).

[53] The plaintiffs in Am. Civil Liberties Union v. Clapper filed their case less than a week after Snowden leaked the Secondary Order of the FISA Court, which revealed the nature and scope of the NSA's Section 215 Telephony Metadata Program (at least as it related to Verizon). *See* Am. Civil Liberties Union v. Clapper, *supra* note 52 at 735. The leaks therefore seem to be the direct cause of the litigation. *See also* Steve Vladeck, *Standing and Secret Surveillance*, 10 I/S: A JOURNAL OF LAW AND POLICY 551, 553 (2014) ("One can certainly question whether Clapper would have come out the same way if [stories driven by the Snowden leaks] had broken prior to the Court's decision.").

[54] Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 791 (2d Cir. 2015).

[55] GOLDSMITH, *supra* note 1, at 84 ("The courts played no role in monitoring CIA activities" during Allen Dulles's time as CIA Director from 1953–61.).

[56] Mohammed v. Jeppesen Dataplan, 614 F.3d 1070, 1072 (9th Cir. 2010) (en banc).

[57] Al-Aulaqi v. Obama, 727 F. Supp.2d 1, 8 (D.D.C. 2010).

[58] R. v. Sec'y of State for Foreign & Commonw. Affairs, [2010] EWCA (Civ) 65, [2010] 3 W.L.R. 554, [14] (Eng.). The U.K. settled the case. *Government to compensate ex-Guantanamo Bay Detainees*, BBC NEWS (Nov. 16, 2010), http://www.bbc.com/news/uk-11762636.

[59] Ravi Somaiya, *Drone Strike Prompts Suit, Raising Fears for U.S. Allies*, N.Y. TIMES (Jan. 30, 2013), http://www.nytimes.com/2013/01/31/world/drone-strike-lawsuit-raises-concerns-on-intelligence-sharing.html (noting that case raised prospect of legal liability for European officials by linking them to U.S. drone campaign, which is widely seen as illegal in their home states). The U.K. Court of Appeal ultimately ruled against Khan. Khan v. Sec'y of State for Foreign and Commonwealth Affairs, [2014] EWCA Civ 24, Jan. 20, 2014, http://justsecurity.org/wp-content/uploads/2014/01/Noor-Khan-v.-State-UK-Court-of-Appeal-2014.pdf.

individual to proceed with his claim that U.K. intelligence services, along with the CIA, rendered him to the Libyan government, which he alleges tortured him.[60]

Savvy plaintiffs have turned to foreign courts when they have failed to achieve victories in their own domestic courts. As Jack Goldsmith writes:

> When the [Center for Constitutional Rights] failed to achieve what it viewed as adequate accountability for Bush administration officials in the United States in connection with detention and interrogation practices, it started pursuing, and continues to pursue, lawsuits and prosecutions against U.S. officials in Spain, Germany, and other European countries. "You look for every niche you can . . . ." said Michael Ratner, explaining the CCR's strategy for pursuing lawsuits in Europe.[61]

Binyam Mohammed's lawyers adopted the same strategy regarding rendition flights: the lawyers first sued Jeppesen in the United States before later suing Jeppesen's U.K. subsidiary.[62] No doubt private plaintiffs (and possibly foreign states themselves) will attempt to use European courts to raise claims against individuals involved in the CIA's interrogation program.[63]

Plaintiffs have also turned to international courts. The European Court of Human Rights (ECtHR) held in *El Masri v. Macedonia* that Macedonia was responsible for the mistreatment of a German national whom the CIA allegedly detained in Macedonia and rendered to Afghanistan.[64] The Court found that in cooperating with the United States Macedonia had violated provisions of the European Convention on Human Rights (ECHR) that prohibited torture and degrading treatment and guaranteed the right to liberty and security. In a separate case, the ECtHR held that Poland had violated the rights of two detainees who the CIA allegedly held and mistreated in secret detention facilities in Poland.[65]

While plaintiffs have not been successful in all of their cases, they have won some. For example, as noted above, the ECtHR held that Macedonia violated

---

[60] Owen Bowcott, *Hakim Belhaj wins right to sue UK government over his kidnap*, THE GUARDIAN (U.K.) (Oct. 30, 2014), http://www.theguardian.com/world/2014/oct/30/abdel-hakim-belhaj-court-kidnap-mi6-cia-torture.

[61] GOLDSMITH, *supra* note 1, at 199.

[62] Ashley S. Deeks, *Litigating How We Fight*, 87 INT'L L. STUD. 427, 441 (2011).

[63] Sophia Pearson, Christie Smythe & Joel Rosenblatt, *Torture-Linked CIA Officials Face Future Stuck in U.S.*, BLOOMBERG NEWS (Dec. 10, 2014), http://www.bloomberg.com/news/articles/2014-12-11/torture-linked-cia-officials-face-future-stuck-on-u-s-; *UN counterterrorism expert says U.S. officials must be prosecuted for CIA torture*, CBC NEWS (Dec. 10, 2014), http://www.cbc.ca/news/world/un-counterterrorism-expert-says-u-s-officials-must-be-prosecuted-for-cia-torture-1.2866895.

[64] Factsheet: Secret Detention Sites, Euro. Ct. Hum. Rts. (July 2014) (describing case of El-Masri v. Macedonia), http://www.echr.coe.int/Documents/FS_Secret_detention_ENG.PDF.

[65] *Id.* (describing Al Nashiri v. Poland and Abu Zubaydah v. Poland).

ECHR Articles 3, 5, 8, and 13 when it facilitated the transfer of Khaled el Masri to U.S. custody.[66] Binyam Mohamed's civil case in the United Kingdom prompted the House of Lords to order the U.K. government to publicly reveal evidence describing what the United Kingdom knew about Mohamed's treatment while in CIA custody.[67] When the results of litigation produce court decisions revealing and restricting IC activity, this alters the legal landscape within which those ICs are operating.[68] This shifting landscape means there is both new law to apply and a public focus on whether and how the ICs are applying that new law.

Finally, litigation is a way for plaintiffs to try to force the government *itself* to directly disclose certain classified information about its IC programs. Through statutes such as the U.S. Freedom of Information Act (FOIA),[69] plaintiffs have filed a number of cases seeking information about intelligence activities, ranging from detention and interrogation to targeted killings.[70] In a number of U.S. cases, advocacy groups and journalists have successfully persuaded courts to order the government to release more than 150,000 pages of previously classified documents that revealed extensive information about intelligence programs.[71] Although plaintiffs have used FOIA for many years to seek information about intelligence activities, the recent number of leaks about intelligence activities means there are more programs about which individuals can (and will) file FOIA requests.[72]

In short, litigation reflects an increasing interest in using the courts to cabin certain intelligence activities. This proliferation of litigation is altering the

---

[66] El Masri v. the Former Yugoslav Republic of Macedonia, App. No. 39630/09, Eur. Ct. H.R. 65–66 (Dec. 13, 2012).

[67] Richard Norton-Taylor, *Binyam torture evidence must be revealed, judges rule*, THE GUARDIAN (U.K.) (Feb. 10, 2010), http://www.theguardian.com/world/2010/feb/10/binyam-mohamed-torture-ruling-evidence.

[68] Cases such as this also shape the broader political and operational environment: in the wake of the *Mohamed* case, the United States reportedly slowed its sharing of sensitive information with the United Kingdom. David Stringer, *Intelligence Ties Between UK and US in Jeopardy*, ASSOCIATED PRESS (Feb. 11, 2010), http://www.boston.com/news/world/europe/articles/2010/02/11/intelligence_ties_between_uk_and_us_in_jeopardy/?page=1.

[69] Freedom of Information Act, 5 U.S.C. § 552 (1966).

[70] Am. Civil Liberties Union v. Dep't of Def., 351 F.Supp.2d 265 (S.D.N.Y. 2005) (granting significant parts of plaintiff's request related to detention and interrogation); N.Y. Times Co. v. U.S. Dep't of Justice, 756 F.3d 100 (2d Cir. 2014) (ordering government to release portion of OLC memorandum on targeted killings).

[71] GOLDSMITH, *supra* note 1, at 116 ("The rise of well-resourced advocacy groups that scrutinize government national security actions . . . is one of the great accountability innovations of the last decade.").

[72] U.S. Department of Justice, Summary of Agency Chief FOIA Officer Reports for 2013 and Assessment of Agency Progress in Implementing the President's FOIA Memorandum and the Attorney General's FOIA Guidelines with OIP Guidance For Further Improvement (July 23, 2014), http://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/2013-cfo-assessment.pdf (stating that the U.S. government faces ever-increasing numbers of FOIA requests).

internal dynamics of ICs, whose activities are affected by the fact of litigation generally and by adverse court holdings in particular.

C. *Legalization*

The litigation just described has led to new case law that regulates ICs. At the same time, disclosures about intelligence activities have also prompted non-judicial actors to impose new rules on ICs directly, either through legislation or executive regulation. On the international plane, these same disclosures have stimulated claims and counterclaims among states, which often take place using the substance and language of international law. This section argues that ICs have become increasingly legalized—that is, infused with law—in the past decade, predominately in terms of increased domestic regulation but also in terms of increasing international regulation.

1. Domestic law

The number of legal officers within the CIA grew around tenfold between the 1970s, when the Agency employed about ten lawyers, and 2010.[73] Accompanying that rise in numbers came a shift in mindset: "the Agency transformed itself from being indifferent to the law to being preoccupied by it."[74] Goldsmith further describes the "scores of legal restrictions on the executive branch" that are enforced by that "bevy of lawyers."[75] By way of example, "Presidential [covert action] findings in the early 1980s used to be very short, but now they are typically many pages long, full of . . . lawyerly caveats 'written for the front page of the *New York Times*' because of expected leaks."[76]

Professor Margo Schlanger has recently written about a comparable phenomenon within the NSA, which she identifies as increased "intelligence legalism."[77] She argues that three developments have produced this legalism: (1) an increased number of substantive rules regulating NSA; (2) some court enforcement of those rules; and (3) empowerment of lawyers within the government.[78] Each of these developments reinforces the others: as the number of rules expands, the need for lawyers to help interpret and apply those rules grows; as the number of lawyers and their role grow, the lawyers become more powerful

---

[73] GOLDSMITH, *supra* note 1, at 87.
[74] *Id.*
[75] *Id.* at 107, quoting in part a senior Department of Justice official.
[76] *Id.* at 89. This further illustrates the connection between the proliferation of leaks and the expanding legalization of ICs.
[77] Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015).
[78] Schlanger bemoans this intelligence legalism on the grounds that it allows policymakers to avoid difficult decisions about whether a given policy is actually the most desirable one from a rights/security perspective. *Id.* at 185–86. I take no view on whether the domestic laws that serve as peer constraints strike the correct rights/security balance, though virtually all of the domestic laws discussed here as peer constraints reflect a shift toward a more rights-protective approach.

players within the IC; and as courts enforce the rules, both the lawyers and the operators will be increasingly attuned to law as a guiding principle for their actions.[79]

ICs outside the United States also have seen themselves increasingly regulated in the past fifteen years. In the United Kingdom, the Regulation of Investigatory Powers Act 2000 structures the way in which public actors in the United Kingdom may conduct surveillance (including communications intercepts), investigations, and the use of covert intelligence sources.[80] Canada's 2001 Anti-Terrorism Act similarly regulates the Communications Security Establishment of Canada (the NSA equivalent) and its collection operations. Moreover, Australia's 2001 Intelligence Services Act provided a statutory basis for the Australian Secret Intelligence Service and Defence Signals Directorate, and imposed requirements of ministerial authorization and parliamentary oversight.[81] This is not to suggest that these states had no intelligence-related statutes on the books before 2000;[82] rather, these examples suggest that these statutes, and more recent amendments to these laws, have become increasingly extensive and detailed.[83] Not all of these new laws are necessarily constraining; indeed, some of the statutes may actually increase the powers of an IC. But often statutes that increase an IC's authority include additional oversight mechanisms and approval procedures. Those latter provisions help build constraints even where the IC's authorities expand.

---

[79] *See, e.g.*, U.K. Foreign Secretary William Hague, Statement to the House of Commons (June 10, 2013), https://www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq. (quoting U.K. Intelligence Services Commissioner's belief that "GCHQ staff conduct themselves with the highest levels of integrity and legal compliance"); President Obama, Remarks by the President on Review of Signals Intelligence (January 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter Obama NSA Speech] ("[N]othing that I have learned since indicated that our intelligence community has sought to violate the law or is cavalier about the civil liberties of their fellow citizens."). *But see, e.g.*, Iain Cameron, *Beyond the Nation State: The Influence of the European Court of Human Rights on Intelligence Accountability*, *in* WHO'S WATCHING THE SPIES? ESTABLISHING INTELLIGENCE SERVICE ACCOUNTABILITY, *supra* note 7, at 34, 36 ("It is evident that in this area the law can serve, and has on occasion served, as a facade, concealing more or less serious divergences in practice.").

[80] Regulation of Investigatory Powers Act, 2000, c. 23 (U.K.) [hereinafter RIPA]. RIPA itself was a reaction to a 1997 decision of the European Court of Human Rights. *See* Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997). The 1989 Security Services Act apparently responded to the fact that the ECtHR had shown a "pronounced distaste for the British habit of relying on unregulated administrative discretion in matters affecting individual rights." Ian Leigh & Laurence Lustgarten, *The Security Service Act 1989*, 52 MODERN L. REV. 801, 803 (1989).

[81] Intelligence Services Act 2001, Act No. 152 of 2001 (Cth) (Austl.).

[82] For instance, the Canadian statute regulating Canada's equivalent of the CIA dates to 1984. *See* Canadian Security Intelligence Service (CSIS) Act (R.S.C., 1985, c. C-23); Security Intelligence Review Committee, "The CSIS Act," http://www.sirc-csars.gc.ca/csiscr/actloi-eng.html.

[83] *See* Aldrich, *supra* note 9, at 35 ("In the 1990s, the European intelligence services went through a regulatory revolution during which many services were given a legal identity and in some cases the European Convention on Human Rights was written into their core guidance.").

The growing role for lawyers in U.K. intelligence operations becomes apparent in oversight reports relating to rendition, interrogation, and detention. The U.K. Parliament's Intelligence and Security Committee's Report on Rendition ("ISC Rendition Report") described how operators receive legal briefings on both domestic and international law to ensure that U.K. intelligence does not result in torture or mistreatment by other ICs.[84] In 2006 the U.K. Security Service, the FBI equivalent, and the Secret Intelligence Service ("SIS"), the CIA equivalent, issued guidance about liaison relationships that recommended when to consult the Service's Legal Advisors.[85] Though the guidance is classified, the cover letter noted, "[The guidance] is a shared document with significant legal input and [] views on some of the legal questions are still evolving. . . . The guidance provides the level of advice which hitherto has been issued by Legal Advisors on a case by case basis."[86] The guidance also advised SIS officers involved in detainee operations to seek legal advice when sharing the location of a person of interest with peer services or receiving information from a peer service that is already detaining someone of interest to SIS.[87] Comparable 2006 guidance for GCHQ employees explained when they should refer to senior management their questions about supplying information, noting that those management officers "would take legal advice as necessary."[88]

In short, ICs have more domestic law to apply, and more lawyers whose job it is to help the relevant agencies apply it. Just as militaries increasingly involve their lawyers in on-the-ground decision-making about targeting and detention, so too do intelligence communities now rely more heavily on their lawyers to provide guidance that affects the nature, scope, and operation of intelligence programs.[89] This development makes particular sense in light of the fact that ICs increasingly are being asked to perform militarized functions. Just as military judge advocates in general are now fully incorporated into military operational decision-making, so too should we expect IC lawyers to begin to play a larger role in navigating comparable intelligence operations.

2. International law

At the same time that ICs increasingly face extensive domestic regulatory regimes, ICs are also beginning to face persistent legal claims derived from a different source: international law. Particularly in the wake of the Snowden leaks,

---

[84] Intelligence and Security Committee, *Rendition* ¶ 174 (July 2007) [hereinafter ISC Rendition Report].
[85] U.K. Detainee Inquiry, *supra* note 46, at 5.79.
[86] *Id.* at 5.83.
[87] *Id.*
[88] *Id.* at 5.92.
[89] *See, e.g.*, GOLDSMITH, *supra* note 1, at 224 ("War has become hyper-legalized, and legality has become the global currency of legitimacy for military and intelligence action."); *id.* at 230 (noting that all significant military and intelligence actions have elaborate, law-heavy pre-clearance processes); Aldrich, *supra* note 9, at 35–36 (noting that ICs spend extensive time arguing with their lawyers before conducting operations).

states and other interested actors increasingly claim that certain intelligence activities violate different aspects of international law. One reason for this is that some states and scholars have a newfound understanding that the activities that some ICs are undertaking—bulk collection of telephonic and internet communications, detention, interrogation, and targeted killings—affect private individuals in ways that earlier forms of intelligence activity did not. After all, ICs are playing a larger role than before in taking forcible actions against individual non-state actors, including during armed conflicts.[90]

Claims that certain intelligence activities violate international law have tended to fall into four categories. First, various states, scholars, and human rights groups have alleged that some of these activities violate the International Covenant on Civil and Political Rights (ICCPR). For instance, some argue that bulk electronic surveillance violates the right to privacy contained in the ICCPR (and, for states parties to the Council of Europe, the ECHR).[91] Until recently, few had considered whether and how governmental electronic surveillance implicated those human rights protections.[92] Others have argued that targeted killings violate

---

[90] *See, e.g.*, Aldrich, *supra* note 9, at 20 (describing intelligence operations today as "more kinetic and more controversial"); U.K. Detainee Inquiry, *supra* note 46, at 5.7 (reciting SIS assertion that before 2001 U.K. SIS was not experienced in interviewing detainees in the field as a result of lack of prior operational need); *id.* at 5.49 (describing how U.K. provided guidance to their IC on Geneva Conventions, based on guidance for U.K. armed forces); Report on the Handling of Detainees by U.K. Intelligence Personnel in Afghanistan, Guantanamo Bay and Iraq, Mar. 1, 2005 [hereinafter ISC Detention Report] at ¶ 89 ("For [the U.K.'s] civilian experts, this was not a new business . . . . I think it is true to say that on this occasion they were closer to the front line, they were more intimately involved with the interrogation process than was our experience in the past . . . .").

[91] *Brazilian President Blasts U.S. for Spying*, XINHUA (Sept. 24, 2013), http://news.xinhuanet.com/english/world/2013-09/25/c_125440237.htm. *See also* Tom Risen, *Brazil's President Tells U.N. That NSA Spying Violates Human Rights*, U.S. NEWS (Sept. 24, 2013), http://www.usnews.com/news/articles/2013/09/24/brazils-president-tells-un-that-nsa-spying-violates-human-rights; Ryan Gallagher, *After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty*, SLATE.COM (Sept. 26, 2013), http://www.slate.com/blogs/future_tense/2013/09/26/article_17_surveillance_update_countries_want_digital_privacy_in_the_iccpr.html (describing Germany's efforts to clarify that the ICCPR applied to electronic privacy); David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013), http://justsecurity.org/2668/foreigners-nsa-spying-rights/; Martin Scheinin, *Letter to the Editor*, JUST SECURITY (Mar. 10, 2014), http://justsecurity.org/8049/letter-editor-martin-scheinin/ (arguing that ICCPR article 17 applies extraterritorially to regulate a state's surveillance of foreign nationals); Amnesty International, *Amnesty International takes UK government to European Court of Human Rights over mass surveillance* (Apr. 10, 2015), https://www.amnesty.org/en/latest/news/2015/04/amnesty-international-takes-uk-government-to-european-court-of-human-rights-over-mass-surveillance/.

[92] *Comments of Human Rights Watch*: *Hearing before the Privacy and Civil Liberties Oversight Board*, (Mar. 19, 2014) (prepared testimony of Laura Pitter, Senior National Security Researcher, Human Rights Watch), at 8, https://www.pclob.gov/events/2014/march19.html (implicitly recognizing lack of clarity in law when stating that "[c]oncepts of jurisdiction based on control over territory and persons . . . can and should adapt to the reality of mass digital surveillance . . . .").

the ICCPR right not to face arbitrary deprivation of life.[93] Second, states have asserted that spying—particularly, electronic surveillance—from within embassies violates the Vienna Convention on Diplomatic Relations.[94] For example, Germany's Foreign Ministry summoned the U.K.'s ambassador to Germany to seek an explanation about reports that the U.K. was spying on Germany from within its embassy in Berlin. The Germany Ministry "indicated that tapping communications from a diplomatic mission would be a violation of international law."[95] Third, states have argued that activities ranging from targeted killings to electronic surveillance violate customary international law norms of sovereignty and territorial integrity.[96] Fourth, most states and scholars accept that the laws of war apply to intelligence activities conducted during armed conflicts. This issue arises because ICs suddenly find themselves operating not only in peacetime situations (e.g., CIA operatives trying to acquire human intelligence on the Kremlin's plans for Russia's nuclear arsenal) but also in wartime situations (e.g., the CIA undertaking targeted killings or detentions of members of Al-Qaeda, a group with which the United States has concluded that it is in an armed conflict). In war, the laws of armed conflict apply; when IC activities take place in the context of an armed conflict, ICs now are expected to comply with that body of law.[97]

While the underlying international rules have long existed and are understood to apply to states' diplomatic, economic, and military activities, states rarely have invoked those rules to contest spying by other states. In fact, only recently have states and other actors made a more systemic push to apply these existing norms more aggressively and with greater specificity to newly revealed

---

[93] ICCPR Art. 6; Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, A/HRC/14/24/Add.6, at ¶¶ 5, 10.

[94] *Pakistan Lodges Protest Against U.S. Surveillance*, KUWAIT NEWS AGENCY (July 4, 2014) (quoting Pakistan Foreign Office release as stating, "The US Embassy in Islamabad was conveyed today that [reported U.S. surveillance] against Pakistani government departments or other organizations, entities and individuals is not in accord with international law and recognized diplomatic conduct").

[95] *Germany Calls in British Ambassador Over Spying Reports*, DEUTSCHE WELLE (Nov. 5, 2013), http://www.dw.com/en/germany-calls-in-british-ambassador-over-spying-reports/a-17204342; Barbara Miller, *Berlin Calls in British Ambassador Over Spying Reports*, ABC (Nov. 5, 2013), http://www.abc.net.au/news/2013-11-06/berlin-calls-in-british-ambassador-over-spying/5072424.

[96] Qasim Nauman & Safdar Dawar, *U.S. Drone Strike in Pakistan Killed Senior Afghan Militant, Others*, WALL ST. J. (June 12, 2014), http://www.wsj.com/articles/u-s-pakistan-drone-strike-targeted-haqqani-network-killing-top-militant-1402578153; United Nations Press Release, *Third Committee Approves Text Titled 'Right to Privacy in the Digital Age,' as It Takes Action on 18 Draft Resolutions*, GA/SHC/4094, (Nov. 26, 2013), http://www.un.org/News/Press/docs/2013/gashc4094.doc.htm (Indonesia claiming that extraterritorial surveillance violates the U.N. Charter, which contains the norms of territorial integrity and sovereignty).

[97] U.K. Detainee Inquiry, *supra* note 46, at 5.49 (describing how U.K. IC was briefed on Geneva Conventions); *id.* at 5.100–101 (describing how SIS staff dealing with detainees received training that included a strong emphasis on legal/human rights issues and how SIS officers received, before deploying to Iraq, briefing on Geneva Conventions, NATO agreements, and the law of armed conflict).

IC activities.[98] We thus can identify both domestic *and* international "intelligence legalism."[99] As a result, ICs are faced with—and must consider—arguments that more bodies of law restrict their activities and may impose additional peer constraints on their partners.

For peer ICs, international law offers a common language and set of norms in a way that domestic law does not. Domestic law often is more detailed and complicated than international law, difficult to apply even by the domestic IC it governs. It may be more difficult for peer ICs to gain familiarity with each others' domestic law than it is to understand the international laws that the peer ICs (and their overseers) apply. The application of international law to IC activities will not always be straightforward, to be sure.[100] After all, at least some states will resist the idea (for instance) that territorial integrity precludes a state from recruiting foreign operatives on foreign soil or collecting by satellite communications by foreign governments. But in jurisdictions where courts or the executives themselves have concluded that particular international norms bind their ICs, those ICs will be constrained by those norms as well as by domestic ones.

Leaks, litigation, and the increasing applicability of legal rules are exposing the nature of IC activities that previously remained secret or were easily deniable; raising questions about the legitimacy of IC activities performed in the name of democratic states; and rendering more law directly applicable to IC activities. This creates a situation in which more ICs come to their liaison relationships with law on their mind, and in which they are positioned, as a matter of choice or necessity, to constrain their peers.

III. Mechanisms of Peer Constraints

There are at least three types of mechanisms by which peer constraints can and do occur: formalized constraints, informal constraints, and public critiques. Although I identify them here as distinct mechanisms, in practice they bleed into and complement each other. Constraints among peer ICs stem from at least two sources. One source of constraints is endogenous to ICs themselves: the communities collectively establish professional rules and norms to guide their own interactions.[101] These norms may do significant work to constrain, but are not

---

[98] The U.K. IC receives a comprehensive legal briefing that addresses the responsibilities of IC staff under U.K. law and U.K. responsibilities under international law. ISC Rendition Report, *supra* note 84, at ¶ 174.

[99] Schlanger, *supra* note 77, at 117 (describing domestic "intelligence legalism").

[100] *See, e.g.*, Deeks, *supra* note 48 (discussing disputes over applicability of various international law principles to spying).

[101] *See* Peter Haas, *Introduction: Epistemic Communities and International Policy Coordination*, 46 INT'L ORG. 1, 3 (1992) (defining epistemic community as a group of professionals with shared normative and principled beliefs; shared causal beliefs; shared notions of validity; and a common policy enterprise).

necessarily driven by or shaped around legal considerations. Rather, they developed to promote the efficiency of intelligence sharing, the accuracy of intelligence products, and the protection of intelligence received from other services.

This article focuses on exogenous sources of constraints: law, policy, and external oversight. It is obvious that the changing legal landscape in a particular state will affect the conduct of that state's IC. The novel point here is that this process, in turn, may cause peer ICs to change their behavior.

Over time, ICs may incorporate these exogenous legal norms into their endogenous norms. If the new legalistic attitudes toward intelligence activities described in Part II continue to infuse the activities of ICs, exogenous concepts such as the inherent value of legal compliance and the close relationship between legal compliance and legitimacy may filter into endogenous professional norms. From an external perspective, it is difficult to know the extent to which this already has happened.[102] Because exogenous concepts are far easier to identify and endogenous norms are opaque to the public, the following discussion focuses on peer constraints that draw from norms of exogenous origin.

The unifying idea among these mechanisms is that they emanate from one state but constrain ICs from other states, which are not *directly* subject to the first state's statutes, judicial decisions, or oversight bodies. Instead, the mechanisms constrain peer ICs *transitively*: in order for the peer relationship between two ICs to function in a particular situation, one peer IC must alter its preferred behavior in order to allow the other IC to continue to cooperate.

A. *Formal Arrangements*

One way that states have memorialized some of the cooperative arrangements discussed in Part I is through relatively formal agreements. A common form of agreement between peer ICs takes the form of "humane treatment assurances."[103] Originally developed in the law enforcement context, these arrangements arise when one state seeks to transfer an individual into another state's custody but fears that the state receiving him may mistreat him.[104] The receiving state may give assurances that it will not engage in certain actions against the transferred individual, and may also allow the sending state or another

---

[102] The adoption of Executive Order 12,333 in the United States in 1981, which mandated various "in-advance" written procedures and warrantless surveillance only with the authorization of the Attorney General, began to move the U.S. IC in a legalistic direction, Schlanger, *supra* note 77, at 132, and by now presumably has infiltrated the endogenous norms.

[103] Some states refer to these as "diplomatic assurances."

[104] *See generally* Margaret L. Satterthwaite, *Rendered Meaningless: Extraordinary Rendition and the Rule of Law*, 75 GEO. WASH. L. REV. 1333, 1379–94 (2007).

entity to have continued access to the person after transfer to monitor his treatment.[105]

This process of obtaining assurances, which often takes place in the context of the extradition or deportation of a person from one state to another, seems to occur in the context of intelligence activities as well. A task force set up by President Obama in January 2009 to examine U.S. policies related to detainee transfers,[106] including those undertaken pursuant to intelligence authorities, recommended that "agencies obtaining assurances from foreign countries insist on a monitoring mechanism . . . to ensure consistent, private access to the individual who has been transferred, with minimal advance notice to the detaining government."[107]

In addition, the task force made classified recommendations designed to ensure that, "should the Intelligence Community participate in or otherwise support a transfer, any affected individuals are subjected to proper treatment."[108] Assuming the executive branch implemented the task force's recommendations, this suggests that the U.S. IC uses assurances to constrain the activities of some other states' ICs. Reports on Canadian IC activities, including those produced in the wake of the rendition of Maher Arar to Syria and his subsequent mistreatment, reflect similar arrangements, which fall under the heading of "caveats" on the use of information.[109] The U.K. IC also seeks treatment assurances in various contexts, including when it is transferring detainees and when it is providing intelligence to a peer service that is likely to lead to human rights abuses by the peer service (which might, for example, use the intelligence to arrest and torture someone).[110] These treatment assurances constitute relatively formal constraints on the conduct of peer ICs.

---

[105] *See* Ashley S. Deeks, *Avoiding Transfers to Torture*, Council on Foreign Relations Special Report No. 35 (June 2008).

[106] E.O. 13,491, 74 Fed. Reg. 4893 (Jan. 22, 2009).

[107] Press Release, U.S. Department of Justice, *Special Task Force on Interrogations and Transfer Policies Issues Its Recommendations to the Presiden*t (Aug. 24, 2009), http://www.justice.gov/opa/pr/special-task-force-interrogations-and-transfer-policies-issues-its–recommendations–president.

[108] *Id*.

[109] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar 30–32 (2006) [hereinafter Arar Report] (describing RCMP use of caveats to preclude peer services that receive intelligence information from using that information for unauthorized purposes).

[110] ISC Rendition Report, *supra* note 84, at ¶ 33 ("Where there are concerns [about detainee treatment], the Agencies seek credible assurances that any action taken on the basis of intelligence provided by U.K. Agencies would be humane and lawful."); U.K. Detainee Inquiry, *supra* note 46, at 5.73; Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas (July 2010) (instructing personnel to consider obtaining assurances from liaison partners as to the standards that have been or will be applied in relation to that detainee to minimize any risk of mistreatment) (cited in U.K. Detainee Inquiry, *supra* note 46, at 3.14).

Another way that states establish the fact of and rules for liaison cooperation is through bilateral intelligence cooperation agreements.[111] Several hundred treaties and agreements regulate cooperation in security and intelligence matters among the Five Eyes states alone.[112] This number grows to over 1,000 when one includes exchanges of letters and memoranda and unwritten understandings concerning the transfer of intelligence information among those states.[113] It is not hard to imagine that many other states have comparable bilateral arrangements with their allies and partners, whether as a way to fill in intelligence gaps, advance political goals, or defend against common enemies.[114] As Richard Aldrich explains, "Intelligence exchange between these organizations is a world within a world, governed by its own diplomacy and characterized by elaborate agreements, understandings and treaties."[115]

While little is known about the contents of these arrangements,[116] one such arrangement recently came to light when Edward Snowden leaked a memorandum of understanding (MOU) between the United States and Israel regarding the sharing of signals intelligence.[117] The MOU requires the Israeli SIGINT National Unit (ISNU) to handle the signals intelligence it receives in accordance with U.S. law (which presumably requires ISNU to minimize any information it receives about U.S. persons) and prohibits Israel from deliberately targeting U.S. persons identified in the data.[118] Further, the MOU requires Israel to destroy upon identification any communication that is to or from a U.S. official, including officials in the Executive, Congress, and the federal courts.[119] It also appears that NSA trains Israeli personnel to protect U.S. person information.[120] If the U.S.-Israel MOU is representative of some of these

---

[111] Section 104A(f) of the National Security Act of 1947 authorizes the CIA Director to "coordinate the relationships between elements of the intelligence community and the intelligence or security services of foreign governments . . . on all matters involving intelligence related to the national security or involving intelligence acquired through clandestine means." E.O. 12,333 gives the Director of National Intelligence the responsibility to "enter into intelligence and counterintelligence arrangements and agreements with foreign governments and international organizations." Exec. Order No. 12,333, 3 C.F.R. 200 (1981), sec. 1.3(b)(4)(A).

[112] RICHELSON & BALL, *supra* note 20, at 141.

[113] *Id.* at 155.

[114] Aldrich, *supra* note 9, at 23 (discussing the "tendency toward 'bilateralism'").

[115] Richard Aldrich, *Transatlantic Intelligence and Security Cooperation*, 80 INT'L AFF. 731, 737 (2004); *see also* ADAM SVENDSEN, INTELLIGENCE COOPERATION AND THE WAR ON TERROR: ANGLO-AMERICAN SECURITY RELATIONS AFTER 9/11 (2010) (identifying MOUs related to human and defense intelligence dating to the 1940s).

[116] Aldrich, *supra* note 9, at 22 n.16 (citing JEFFREY RICHELSON, THE U.S. INTELLIGENCE COMMUNITY 280–81 (2d ed. 1989)). In general, more formal versions of these arrangements often specify that the parties cannot recruit each other's citizens as agents or operate on each other's territory without permission.

[117] Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA shares raw intelligence including Americans' data with Israel*, THE GUARDIAN (U.K.) (Sept. 11, 2013), http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[118] *Id.*

[119] *Id.*

[120] *Id.*

cooperative agreements, it illustrates that states are—at least within certain limits—willing to agree at some level of formality to conform their behavior to peer requirements to accomplish shared goals.

U.S.-Russian arms control agreements provide a final example of a situation in which states have formalized their intelligence agreements. Somewhat surprisingly, the United States and Russia have agreed to allow each other to conduct certain forms of spying as a way to ensure compliance with arms control commitments. In several bilateral arms control treaties, each party undertakes "to use national technical means of verification at its disposal in a manner consistent with generally recognized principles of international law," "not to interfere with the national technical means of verification of the other Party," and "not to use concealment measures that impede verification, by national technical means . . . of compliance with the provisions of this Treaty."[121] These provisions effectively constrain the parties from attempting to block spying by the other for verification purposes. Though the provisions impose constraints on the *inhibition* of spying, rather than the *conduct* of spying, these types of arrangements further suggest that states are willing to use formal arrangements to constrain their own ICs.[122]

The extent to which the constraints imposed by these formal arrangements are overtly or secondarily driven by legal concerns admittedly is difficult to determine. In view of the legalization phenomenon assessed in Part II, however, it seems highly likely that IC lawyers are involved in drafting these more formalized arrangements—at least now, if not in earlier eras—and that they would ensure as a matter of course that their contents are consistent with their own states' legal obligations. If so, these formal arrangements may incorporate peer legal constraints, whether explicitly or implicitly.

B. *Informal Mechanisms*

Perhaps the most important and unexplored constraining mechanisms are more informal, based on private peer influence and driven by the domestic and international legal constraints of peer states. These constraints are not captured in written agreements; instead, they emerge from inter-service discussions and atmospheric concerns about legal compliance. These informal mechanisms take four basic shapes: (1) actual legal constraints on one peer IC that alter the behavior of other peer ICs; (2) anticipated legal or regulatory changes that instill preemptive caution in one peer and then shift that caution to another peer; (3) aggressive external oversight of one IC that alters the operational calculations in

---

[121] Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms ("New START"), U.S.-Russ., art. X, Apr. 8, 2010, S. Treaty Doc. No. 111-5, 2010. *See also* Treaty on the Elimination of Intermediate-Range and Shorter-Range Missiles, U.S.-U.S.S.R. ("INF Treaty"), art. XII, Dec. 8, 1987, S. Treaty Doc. No. 100–11, 1988.

[122] The Five Eyes arrangement, which does not speak directly to compliance with domestic or international law, also evidences a willingness by each member's IC to self-constrain in order to facilitate intelligence-sharing among close allies.

that IC's relationship with its peer ICs; and (4) face-to-face influence among peer ICs as intelligence operations transpire on the ground.

1. Peer domestic legal constraints

The paradigmatic informal peer IC constraint arises when two ICs seek to cooperate and one state, by virtue of its international or domestic legal obligations, imposes a condition on the cooperation that alters how the other state behaves. The legal obligations on the first IC may flow from statute, treaty, customary international law, or case law. This sub-section offers two specific examples of peer domestic legal constraints, to illustrate when and how ICs can constrain each other. One example explores the type of constraints the United Kingdom imposed on U.S. detention, interrogation, and rendition in the latter's conflict with Al-Qaeda. The second features Germany's constraints on U.S. targeting of members of Al-Qaeda and associated forces. The subsection then highlights comparable forms of constraint that appear in the military and law enforcement contexts as further suggestive evidence that peer constraints exist in the IC arena.

a) Direct evidence of constraint

i. U.K. restraints on U.S. detention, interrogation, and rendition.

In the wake of revelations that the United Kingdom's IC was involved—directly and indirectly—in U.S. activities such as detention, rendition, and interrogation in Afghanistan, Iraq, and Guantanamo, the ISC undertook several investigations of the U.K.'s participation in these activities.

As background, the U.K. legal obligations potentially implicated by these actions derive from a number of sources. Under the Convention Against Torture ("CAT"), the United Kingdom has an obligation to not knowingly assist in sending a person to another country (including by rendition) where there is a real risk that he may be tortured.[123] Pursuant to the ECHR and the CAT, the U.K. may not treat detainees in an inhuman or degrading manner (which the ECtHR has interpreted to mean that the acts complained of are such as to arouse in the applicant feelings of fear, anguish, and inferiority capable of humiliating and debasing him).[124] For the United Kingdom, this includes the use of hooding and "wall-standing."[125] The United Kingdom also must affirmatively act to forestall any act of torture it can foresee.[126] Finally, the United Kingdom is not permitted to participate in renditions to bring individuals to the U.K.[127] One ISC report

[123] ISC Rendition Report, *supra* note 84, at ¶ 13.
[124] *Id.* at ¶ 15.
[125] ISC Detention Report, *supra* note 90, at ¶ 26.
[126] ISC Rendition Report, *supra* note 84, at ¶ 16.
[127] *Id.* at ¶ 11.

asserts that "UK Agencies have always been mindful of human rights issues, particularly when engaging with countries that do not pay the same attention to civil liberties and human rights as the UK."[128]

The ISC reports, taken as a whole, lead to the conclusion that the U.K. IC has repeatedly imposed informal legal constraints on U.S. IC activities. It has done so in particular through the use of caveats on information it shares with the United States, driven by U.K. legal obligations that often do not apply as a matter of black letter law to the United States.[129] For example, where there are concerns about what a partner IC will do with an individual if the United Kingdom shares information about that individual with the partner IC, "the Agencies seek credible assurances that any action taken on the basis of intelligence provided by the UK Agencies would be humane and lawful."[130] Even before the September 11 attacks, the United Kingdom sought assurances from the U.S. IC when it provided certain types of intelligence to the United States, to minimize the risk that the United States would use that intelligence to target the subject of the rendition using lethal force or subject him to the death penalty.[131] This was true even when a very high profile terrorist such as Osama Bin Laden was the target of a U.S. rendition to bring him to trial in the United States. Though the ISC Rendition Report is not entirely clear about whether the U.S. IC provided humane treatment assurances to the United Kingdom in particular cases, the United Kingdom clearly was prepared to condition the intelligence it shared with the United States on the receipt of those assurances.[132]

---

[128] *Id.* at ¶ 31.

[129] *Id.* at ¶ U (describing twenty-year use of caveats placed on intelligence and honored by the United States).

[130] *Id.* at ¶ 33. Although this article also discusses diplomatic assurances under the heading of "formal arrangements," it seems likely that ICs seek and receive at least some of these treatment assurances on a more informal basis, so they are discussed here as well. *See also* Arar Report, *supra* note 109, at 33 (expressing view that Royal Canadian Mounted Police must only provide information to liaison services in way that minimizes invasions of human rights); Keenan Mahoney et al., *NATO Intelligence Sharing in the 21st Century*, Columbia School of Int'l and Pub. Aff. Capstone Report (Spring 2013), at 27, https://sipa.columbia.edu/sites/default/files/AY13_USDI_FinalReport.pdf ("Another potential obstacle to intelligence cooperation with Germany is the concern over German intelligence being used for purposes that are not acceptable within the framework of German law. Examples of such activities include the death penalty, targeted killings, or interrogation methods that German law does not allow.").

[131] ISC Rendition Report, *supra* note 84, at ¶ 38. The U.K. also appears to have sought assurances from other foreign ICs regarding the treatment of those rendered to stand trial. Those assurances were kept. *Id.* at ¶ 79.

[132] *Id.* at ¶¶ 40–41. *See also* Arar Report, *supra* note 109, at 31 (recommending that Canadian IC should impose caveats on the use of Canadian intelligence in every situation). The Canadian Government has stated that it accepted 22 of the 23 recommendations contained in the Arar Report. Government Response to the Report of the Standing Committee on Public Safety and National Security, Government of Canada, Review of the Findings and Recommendations Arising from the Iacobucci and O'Connor Inquiries, http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4144670&Language=E&Mode

This was not the only context in which the United Kingdom sought assurances from the United States. On occasion, the United Kingdom transmitted questions to the U.S. IC for the United States to ask individuals in U.S. custody. In these cases, the United Kingdom sought assurances that the United States would not subject the detainees being interrogated to torture or cruel, inhuman, or degrading treatment.[133] Although the ISC Rendition Report does not describe what commitments the United States made in response, the report states that after September 11 "greater use was made of assurances with the Americans."[134]

This practice is not limited to the U.K.-U.S. relationship. The U.K. Security Service told the ISC that its humane treatment safeguards apply globally:

> [S]uch conditions are understood by intelligence and security services globally, as they all use similar conditions to ensure that one agency does not endanger another agency's sources through their incautious use of intelligence. Intelligence and security services accept and respect these conditions because failure to do so would mean that they might not be trusted to receive intelligence in the future.[135]

The United Kingdom also has placed strict restrictions on when the United States may use U.K. airbases or airspace for renditions.[136] In some cases, refusals like these work as affirmative constraints—as where the use of U.K. airspace presents the only option for the United States to execute an operation. In that case, the United States would be unable to complete its mission. In other cases, this type of refusal simply increases the transaction costs for the United States, because the U.S. government must find alternative routes or methods by which to

---

=1&Parl=40&Ses=2. The Government reports that "CSIS has pursued a number of important initiatives to improve its information handling practices, including: amending operational policy governing information-sharing and cooperation to restate the need to take the human rights record of a country into account before sending or using information from that country; conducting assessments of the human rights records of the countries and agencies with which it exchanges information; and introducing a new caveat to information it shares with foreign agencies that seeks assurances that any Canadian citizen detained by a foreign government will be treated in accordance with the norms of relevant international conventions." *Id.*

[133] ISC Rendition Report, *supra* note 84, at ¶ 74. The U.K. IC also conveyed to Afghan interlocutors that detainees must not be mistreated and that SIS officers "must act according to UK laws on the matter, which were strict." U.K. Detainee Inquiry, *supra* note 46, at 5.21.

[134] ISC Rendition Report, *supra* note 84, at ¶ 74.

[135] *Id.* at ¶ 171.

[136] *See, e.g.*, David Miliband MP, Secretary of State, *Written Ministerial Statement to the House of Commons*, HOUSE OF COMMONS FOREIGN AFFAIRS COMMITTEE: BRITISH FOREIGN POLICY AND THE ARAB SPRING: SECOND REPORT OF SESSION 2012–13 (3 July 2008, col 58WS) https://books.google.com/books?id=oR_12687HE0C&pg=PA80&lpg=PA80&dq=united+states+use+united+kingdom+airspace+render+detainees&source=bl&ots=VEwq-cooWF&sig=G2IOMYJmpzLCyK2uQJLVzLkIA14&hl=en&sa=X&ved=0ahUKEwi66JyRlL7JAhWGcD4KHV7OB20Q6AEIKTAC#v=onepage&q=united%20states%20use%20united%20kingdom%20airspace%20render%20detainees&f=false, at 82.

conduct an operation. The ISC Rendition Report states, "The U.S. rendition programme has required that the Security Service and SIS modify their relationship with their American counterparts to ensure that, in sharing intelligence, the differing legal frameworks of both countries are honoured."[137] In some cases, this may mean that the United States attempted to work around U.K.-imposed constraints, perhaps by obtaining relevant intelligence from other, less-constrained sources, or by seeking to use airports or facilities of less-constrained ICs. In other cases, however, in which the U.S. IC needed to continue to work with the U.K. IC, the U.S. IC would have had to modify its behavior. The ISC Rendition Report states that certain renditions involving individuals who lived in the United Kingdom or who were believed to possess intelligence about terrorist activity in the United Kingdom "were dropped by the Americans after the [Security] Service had expressed concern at the proposal."[138]

ii. German constraints on U.S. targeting.

Peer constraints related to targeting, particularly of members of Al-Qaeda outside of the Afghan theater, also exist and are likely to expand in the future. This is due in part to different perceptions between the United States and a number of its allies about whether it is legally accurate to characterize the use of force against Al-Qaeda as part of an armed conflict or whether, instead, it is properly characterized as a law enforcement-type operation.

In 2011, German intelligence officials informed their U.S. counterparts about a German citizen in Pakistan who had bragged about planning a suicide attack, and gave the U.S. IC his cell phone number and the address of a café in Mir Ali that he frequented.[139] The United States reportedly used that information to target and kill the German citizen in a drone strike.[140] Germany's Interior Ministry subsequently instructed Germany's domestic intelligence service to stop providing U.S. intelligence officials with information that would enable them to locate German citizens and use force against them.[141] As one analysis states, "[T]here are major concerns with German information being used for purposes that are considered unethical or illegal at home."[142] Further, when providing non-locational information to the U.S. IC, the German intelligence agencies caveat the use of that information, such that the United States only may use it to arrest (not

---

[137] ISC Rendition Report, *supra* note 84, at ¶ 157.
[138] *Id.* at ¶ 158 (citing Oral evidence—Security Service, 23 November 2006).
[139] Holger Stark, *Drone Killing Debate: Germany Limits Information Exchange with US Intelligence*, DER SPIEGEL ONLINE (May 17, 2011), http://www.spiegel.de/international/germany/drone-killing-debate-germany-limits-information-exchange-with-us-intelligence-a-762873.html.
[140] *Id.*
[141] *Id*.
[142] Mahoney et al., *supra* note 130, at 26 (also noting that "Germans place a high premium on ethical standards in foreign policy, and their concern for human rights is a stronger driving force than many foreign observers realize.").

kill) suspected terrorists.[143] Assuming the United States continues to receive information from the Germans about German citizens in areas outside of the Afghan theater, the United States thus faces a peer constraint on how it uses that information, even though its own domestic laws and interpretation of international legal rules might allow it to target the individual using lethal force.[144]

b) Parallel constraints in partner military and law enforcement operations

It should come as no surprise that peer constraints exist among ICs. After all, peer constraints—some overt, and others made public through leaks—can be found in several other areas that directly implicate national security. Specifically, in any number of situations, one state's domestic law constrains how that state may cooperate with peer state agencies to pursue military or law enforcement operations or goals. A few examples suffice.

In the context of military coalitions, peer constraints abound. During the NATO action in Kosovo, which involved air strikes against Yugoslav and Serbian forces, "the byzantine American procedures for approving targets needed to be replicated by every NATO government and its lawyers."[145] That means that each target that NATO bombed had to meet the highest common denominator of acceptability among the twenty-eight NATO states. Thus, a state that interpreted law of war targeting rules particularly narrowly could "turn off" a proposed target that did not comply with that narrow interpretation. That is an example of a broad peer constraint.

Similar constraints exist in the context of weapons bans and sales. For instance, the United States constrained the Israeli government's use of cluster munitions as a condition of selling those weapons to Israel.[146] The United States has insisted that Israel only use cluster munitions against organized Arab armies and, notably for legal purposes, only against clearly defined military targets and not in areas where civilians are known to be present or in areas normally inhabited by civilians.[147] The U.S. government has also required Israel to provide it with

---

[143] Stark, *supra* note 139.

[144] The United States has concluded that it may, consistent with U.S. and international law, target members of Al-Qaeda in various locations as part of its armed conflict with that group. *See* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, *The Obama Administration and International Law* (Mar. 25, 2010), http://www.state.gov/s/l/releases/remarks/139119.htm.

[145] GOLDSMITH, *supra* note 1, at 132. *See also* Spiegel Staff, *Obama's Lists: A Dubious History of Targeted Killings in Afghanistan*, DER SPIEGEL ONLINE (Dec. 28, 2014), http://www.spiegel.de/international/world/secret-docs-reveal-dubious-details-of-targeted-killings-in-afghanistan-a-1010358.html (noting that Germany repeatedly urged its allies in ISAF to remove suspects from the targeting list because it used a higher legal standard for who it could kill).

[146] Jeremy Sharp, Cong. Research Serv., RL33222, *U.S. Foreign Aid to Israel* 10–11 (2009) (describing instances in which United States restricted aid or rebuked Israel for possible improper use of American-supplied cluster munitions).

[147] Bonnie Docherty et al., Human Rights Watch, Flooding South Lebanon: Israel's Use of Cluster Munitions in Lebanon in July and August 2006 103 (Feb. 2008), http://www.hrw.org/sites/default/files/reports/lebanon0208webwcover.pdf; David Cloud, *Inquiry*

information about its cluster munitions use to assist in the cleanup of unexploded munitions resulting from Israel's use of that weapon.[148] These constraints, which are widespread in the arms export control area, are intended to tighten the rules of use beyond the rules that ordinarily would apply directly to the state employing the weapon.

Peer constraints also pervade international law enforcement cooperation. One common example appears in extradition relationships: states parties to the ECHR cannot extradite an individual to a state that may impose the death penalty on him.[149] At one point, Mexico could not extradite individuals to the United States where those individuals faced life imprisonment without parole, even though life without parole is a lawful penalty in the United States.[150] Similarly, the United States constrained the Government of Colombia when Colombia wanted to restart a program under which it employed lethal force against aircraft used to traffic narcotics (and needed U.S. assistance to identify those aircraft). A U.S. statute provided that the United States could only assist such programs where the President certified that interdiction of aircraft reasonably suspected to be primarily engaged in illicit drug trafficking in a particular country's airspace was necessary because of the extraordinary national security threat posed to that country, and that the country had appropriate procedures in place to protect against the loss of innocent life, including effective means of identifying and warning aircraft.[151] As a result, Colombia had to agree to extensive precautions governing its interception of suspicious aircraft before it could use lethal force against those aircraft.[152] U.S. law therefore directly affected how Colombia could

---

Opened Into Israeli Use of U.S. Bombs, N.Y. Times (Aug. 25, 2006), http://www.nytimes.com/2006/08/25/world/middleeast/25cluster.html?_r=0. *See also* U.S. Dep't of State, Office of the Spokesperson, *U.S. Export Policy for Military Unmanned Aerial Systems* (2015) (stating that United States will require purchasers of U.S.-manufactured drones to "use these systems in accordance with international law, including international humanitarian law and international human rights law, as applicable" and use them "in operations involving the use of force only when there is a lawful basis for use of force under international law, such as national self-defense").

[148] Int'l Comm. of the Red Cross, Expert Meeting Report: Humanitarian, Military, Technical and Legal Challenges of Cluster Munitions 14 (Apr. 2007) (describing a secret agreement between the United States and Israel outlining restrictions on Israel's use of cluster munitions, which Israel violated, leading to an eight-year ban on sales by the U.S. government of those munitions to Israel).

[149] Soering v. United Kingdom, 161 Eur. Ct. H.R. (ser. A) (1989) (holding that the United Kingdom could not extradite Soering to the United States because the very long time spent by those on death row in the United States exposes that individual to a real risk of inhuman or degrading treatment).

[150] *Mexico alters extradition rules*, BBC NEWS (Nov. 30, 2005), http://news.bbc.co.uk/2/hi/4483746.stm (describing Mexican Supreme Court's reversal of four-year ban on extraditions to face life without parole).

[151] 22 U.S.C. § 2291–4.

[152] U.S. Gov't Accountability Office, GAO-05-970, Air Bridge Denial Program in Colombia Has Implemented New Safeguards, but Its Effect on Drug Trafficking Is Not Clear (2005) (describing program and letter of agreement between the U.S. government and Colombia regarding program's safety requirements and operational procedures).

conduct its program, even though the Colombian government was not governed by that U.S. statute and Congress could not have regulated Colombia directly even if it wanted to.[153]

As the density of laws regulating the IC and the number of IC lawyers increase, it is predictable that IC peer constraints will flourish (though less publicly) in ways comparable to their cousins in the military and law enforcement contexts. Western militaries and law enforcement agencies today are infused with lawyers—certainly in a more public way than ICs, and in far higher numbers.[154] Quoting General James L. Jones, Charles Dunlap writes, "It used to be a simple thing to fight a battle. . . . [b]ut that's not the world anymore. . . . [Now] you have to have a lawyer or a dozen. It's become very legalistic and very complex."[155] Just as fighting wars has become more legally complex, conducting intelligence activity requires states to grapple with more and more complex laws. As a result, we should expect that ICs will face peer constraints comparable to those that arise in military contexts.

2. The observer effect

When crafting IC policies, states are not guided solely by the laws on the books. States also craft policies in anticipation of litigation. The threat of having a court adjudicate and reject a national security policy gives executive branches an important incentive to render those policies more rights-protective, even before the court weighs in.[156] This phenomenon, which I have termed elsewhere the "observer effect," occurs particularly when three elements are in place.[157] First, there must be a triggering event, which often means that a court has become seized with a national security case after an extended period of non-involvement in security issues.[158] Second, the executive must face robust jurisdictional or substantive uncertainty, leaving it unsure whether a court will take jurisdiction over a given national security-related case, or unsure how a court will rule on the merits if it hears the case.[159] Third, the executive is more likely to alter a policy when it perceives a high likelihood of future litigation on related issues.[160] Courts can also express their displeasure with various policies even if they uphold those policies as a legal matter;[161] critical language in a court opinion can increase the

---

[153] Brazil's shootdown program is subject to the same constraints. *See* H.R. DOC. NO. 111-89 (2010).
[154] GOLDSMITH, *supra* note 1, at 125 ("Until recently, however, lawyers did not play a large role in war-fighting.").
[155] Charles Dunlap, *Legal Issues in Coalition Warfare: A US Perspective*, 82 INT'L L. STUD. 221, 221 (2006).
[156] *See generally* Ashley S. Deeks, *The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference*, 82 FORDHAM L. REV. 830 (2013).
[157] *Id.*
[158] *Id.* at 835.
[159] *Id.* at 838.
[160] *Id.* at 840.
[161] N.Y. Times Co. v. Dep't of Justice, 915 F. Supp. 2d 508, 515 (S.D.N.Y. 2013) (expressing

executive's uncertainty about future litigation outcomes. As a rational actor that seeks to retain maximal control over policy-setting, the executive often responds to these three elements by shifting its policy to a position that gives it more confidence that courts would uphold the policy if hearing the case on the merits.[162]

Intelligence activities are prime candidates for the observer effect. As described above, many of these activities for decades have remained free from court challenge or judicial regulation. Yet this has changed in the past several years, with courts recently taking jurisdiction over cases related to surveillance, renditions, detainee treatment, and targeted killings. As a result, executive branches now, as never before, are aware that courts may step in to review their intelligence activities, and they thus now have far greater incentives to structure those activities with potential judicial oversight in mind.

When the observer effect operates on a single state and its IC, the state may craft its intelligence policies to be less aggressive than its domestic law might allow on its face. When a given state crafts its IC policies more narrowly as a result of the observer effect, this can translate into increased constraints on peer ICs.[163] That is, the state operating under the observer effect will conclude that it has less leeway to conduct a particular intelligence activity, which may increase the quantum of constraint that it imposes on its peer ICs.

How has this operated in the real world? Consider the Anwar Al-Aulaqi litigation.[164] Al-Aulaqi's father sought an injunction prohibiting the U.S. government from killing his son, a suspected operational leader of Al-Qaeda, unless Al-Aulaqi presented a concrete and imminent threat and there was no other way to suppress the threat.[165] As an initial matter, the United States presumably did not anticipate that its targeted killing policies would end up in court, given their level of classification. Although the district court judge in the Al-Aulaqi case held for the government, the judge expressed real discomfort with the targeted killing policy.[166] The U.S. government subsequently issued documents explaining its targeted killing policy, which authorized a far narrower set of killings than the operative U.S. legal theory would have permitted.[167] The U.S. government may

---

concern about the "Alice-in-Wonderland nature" of the dilemma the court faced in weighing secrecy against democracy); Al-Aulaqi v. Obama, 727 F. Supp. 2d 1 (D.D.C. 2010).

[162] Deeks, *supra* note 156, at 840–41.

[163] It is not clear as a general matter whether there is an overall net gain or net loss when ICs operating in gray areas act less aggressively than the law allows. Excessive caution may impose costs, though those costs are nearly impossible to calculate. GOLDSMITH, *supra* note 1, at 231.

[164] *See Al-Aulaqi*, 727 F. Supp. 2d 1.

[165] *Id.*

[166] *Id.*

[167] White House Office of Press Sec'y, Fact Sheet: U.S. Policies and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities (May 23, 2013), https://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism.

have publicized this policy in part to affect the outcome of future litigation about targeting. In any case, it revealed a narrower intelligence policy than U.S. law might require, crafted in the shadow of the observer effect.

U.K. courts have triggered the observer effect inside the U.K. government. Even though a court ultimately dismissed Noor Khan's lawsuit related to targeted killings in Pakistan,[168] the U.K. IC remains nervous about future judicial ramifications of transmitting information to the United States. As a reporter notes, "[I]n light of Mr. Khan's lawsuit and the potential for others, operatives across the British intelligence agencies are concerned that if they share information [with the United States], they could be 'punished by the judiciary for something the executive ordered them to do.'"[169] Further, the *Khan* court stated, "I accept that it is certainly not clear that the defence of combatant immunity would be available to a UK national who was tried in England and Wales with the offense of murder by drone strike."[170] Statements such as this are likely to leave lingering concerns in the minds of officials whose tasks involve collecting or sharing intelligence that could be used to conduct drone strikes away from hot battlefields. More generally, the quantum of litigation in Europe has created penumbral concerns about operating in areas where the legal rules and precedents are not clear-cut, such as in bulk electronic data collection and counterterrorist operations. Knowing that these courts are sympathetic to the idea of extending human rights rules to armed conflict and intelligence activities necessarily will prompt states to be cautious when developing policies that may be in some tension with human rights principles.[171]

In sum, the newfound role for courts in evaluating intelligence activities, coupled with untested legal principles and fear of further leaks[172] that may prompt additional litigation, have produced an atmosphere in which executive branches, including ICs, may self-constrain in ways that translate into additional peer constraints.

3. External oversight of peer ICs

Relatedly, if one partner state faces aggressive domestic oversight or its citizens have robust access to courts, that state may choose to avoid certain types of controversial cooperation with IC partners because it fears that the cooperation

---

[168] Khan v. Sec'y of State for Foreign & Commonwealth Affairs, [2014] EWCA (Civ) 24 [19].
[169] Somaiya, *supra* note 16.
[170] Khan, *supra* note 168, at ¶ 19.
[171] Deeks, *supra* note 62, at 448.
[172] One of the CIA's own internal recommendations for future operations in response to the SSCI Report anticipates future leaks, stating that the CIA should "[b]etter plan covert actions by addressing at the outset the implications of leaks . . . ." CENT. INTELLIGENCE AGENCY, CIA COMMENTS ON THE SENATE SELECT COMMITTEE ON INTELLIGENCE'S STUDY OF THE CENTRAL INTELLIGENCE AGENCY'S FORMER DETENTION AND INTERROGATION PROGRAM 17 (June 27, 2013), https://www.cia.gov/library/reports/CIAs_June2013_Response_to_the_SSCI_Study_on_the_Former_Detention_and_Interrogation_Program.pdf.

will be revealed in one of those fora. For instance, the proliferation and not infrequent success of U.K. litigation, much of which is connected to U.S.-U.K. cooperation, is likely to heighten U.K. caution when working with the United States on sensitive issues because the political, financial, and resource-related costs to the United Kingdom have proven high, even when plaintiffs lose.[173] Conversely, the partners of a heavily-overseen IC may fear that their cooperation will be revealed through the first state's oversight mechanisms and be more hesitant to cooperate *ex ante*. These chilling effects serve as peer constraints because the circumstances surrounding the operations of one IC alter the behavior of a peer IC, including in ways that will be rights-protective.[174]

U.K. courts have proven quite willing to adjudicate the legality of U.K. detentions (regardless of location), treatment of detainees, and renditions.[175] As a result, both the U.K. and U.S. ICs are aware that the United Kingdom has a robust and relatively aggressive external oversight mechanism in the form of judges. This means that the U.K. IC is likely to think long and hard about the likelihood of being sued for particular actions, and the U.S. IC is likely to think hard about the cost of cooperating with the United Kingdom in a particular case, which costs might include disclosures in U.K. courts of certain U.S. intelligence activities. For example, a U.K. court required the U.K. executive to release seven paragraphs related to the alleged mistreatment of Binyam Mohamed.[176] A different U.K. court decided to allow a case to proceed that involves allegations that the SIS and CIA rendered a Libyan named Belhaj to Libya for harsh questioning.[177] It seems likely that the U.K. executive will face pressure in that case to reveal information that might implicate U.S. intelligence activities.

---

[173] Deeks, *supra* note 62, at 447.

[174] There surely will be cases in which State X simply declines to share intelligence with State Y, a peer IC that faces extensive external oversight. That would not be a constraint in the way this article uses that term, though it would alter the behavior of State X and, as a result, the behavior of State Y (because the latter would lose an opportunity to act on a particular piece of intelligence).

[175] Al Skeini et al. v. Sec'y of State for Defence, [2007] UKHL 26, [2008] 1 A.C. (H.L.) [153] (appeal taken from Eng.); R. (on the application of Al-Jedda) v. Sec'y of State for Defence, [2007] UKHL 58, [2008] 1 A.C. 332 (appeal taken from Eng.); The Queen (on the application of Maya Evans) v. Sec'y of State for Defence, [2010] EWHC 1445 (Q.B.) (U.K.); Serdar Mohammed v. Ministry of Defence, [2014] EWHC 1369 (QB). This stands in contrast to U.S. courts, which have concluded that they will adjudicate the legality of detentions only at Guantanamo and not those in more active areas of hostilities such as Afghanistan. In further contrast to U.K. courts, U.S. courts have also rejected treatment claims and have upheld U.S. transfers to other states in the face of claims of anticipated mistreatment post-transfer. Al Maqaleh v. Gates, 605 F.3d 84 (D.C. Cir. 2010) (refusing to assess legality of U.S. detentions in Afghanistan); Doe v. Rumsfeld, 683 F.3d 390 (D.C. Cir. 2012) (granting qualified immunity to Secretary of Defense for alleged mistreatment of detainee); Munaf v. Geren, 553 U.S. 674, 688 (2008) (deferring to Executive's determination that detainees would not face torture upon transfer to Iraqi government).

[176] Mohamed v. Sec'y of State for Foreign and Commonwealth Affairs, [2010] EWCA (Civ) 65, [2011] QB 218.

[177] Belhaj & Boudchar v. Straw & Others, [2014] EWCA (Civ) 1394.

U.K. courts continue to involve themselves in intelligence issues notwithstanding the fact that the U.K. executive has made clear that it objects to having its courts pass judgment on U.S. conduct. For example, in the *Khan* case, the U.K. government argued that the court should find the case non-justiciable because:

> the Court itself[] would necessarily have to make a series of determinations regarding the conduct of the Governments of third States (both the United States and Pakistan). In particular, the Court would have to reach conclusions as to whether the conduct of the United States, and members of the US Administration, amounted to serious violations of international law and criminal law.[178]

The U.K. executive went on to note that "[t]here is a strong risk that any findings or assumptions by a U.K. court in this case would cause the US to revisit and perhaps substantially modify the historic intelligence sharing relationship and national security cooperation."[179] Notwithstanding these asserted concerns, in some cases the U.K. courts have forced disclosure. The ICs of the United Kingdom and United States now are aware that the information they exchange might be at risk of release to a court—and ultimately the public—especially when that information implicates legally contentious activities.[180]

Courts are not the only entities that oversee IC activities: some non-judicial overseers have been particularly active in the wake of the September 11 attacks, producing reports that describe in detail the activities both of their domestic ICs and the actions of some liaison ICs. For example, the breadth and depth of ISC reporting on U.K. intelligence activities suggests that both the United Kingdom and its peer ICs are on notice that many of the United Kingdom's activities (and the shortcomings of both the United Kingdom and its peers) may be revealed in ISC reports.[181] The ISC Detention Report reflects multiple criticisms of U.S. detention practices, discussed in the context of

---

[178] Khan, *supra* note 168, at ¶ 22.

[179] *Id.* at ¶ 23. The United Kingdom made similar submissions in the Binyam Mohamed case, where it asserted that revealing the intelligence information from the United States would be "profoundly damaging to the interests" of the United Kingdom, particularly in light of the fact that the United States had asserted that the release of that information would adversely affect the U.S.-U.K. intelligence relationship. *See* Deeks, *supra* note 62, at 440, 447 (quoting then-State Department Legal Adviser John Bellinger as stating that the "public disclosure of these documents is likely to result in serious damage to US national security and could harm existing intelligence information-sharing arrangements between our two Governments").

[180] *See* Deeks, *supra* note 62, at 447. *See also Belhaj*, *supra* note 177 (rejecting Her Majesty's Government's invocation of act of state doctrine and concerns about litigation that would force it to release U.S. intelligence).

[181] Additionally, Germany has strong parliamentary oversight over its intelligence services. Mahoney et al., *supra* note 130, at 22 (discussing Parliamentary Control Committee and G10 Committee).

evaluating U.K. officials' reaction to those practices.[182] The independent report was produced by Sir Peter Gibson, a retired senior U.K. judge, who reportedly had access to 20,000 documents, many of which were highly classified.[183] Even though some parts the ISC and Gibson reports were redacted, both reports contained extensive discussions of activities that previously had not been officially disclosed. The SSCI Report on the CIA's detention and interrogation program likewise contains new, detailed discussions of U.S. interrogations and the use of secret sites in other countries, something that the U.S. IC worries will erode the trust of liaison services that agreed to cooperate with the United States based on an expectation of secrecy.[184] Finally, some states have agreed to allow international human rights bodies to accept individual complaints. Even though the monitoring bodies "do not comment directly on compliance" by liaison services, these "proceedings . . . nevertheless . . . [publicize and record] the facts and circumstances" of actions such as renditions by the subject state, which may include interactions with peer ICs.[185]

4. Direct operational influence

In addition to the higher-level constraints described in the prior sections, another level of constraint may occur when IC operators actually execute the activities originally negotiated among IC officials higher up the chain of authority. For example, for several months in 2004, U.K. personnel were embedded with U.S. personnel at a U.S. detention facility in Iraq, a position that gave them direct exposure to U.S. operations.[186] The U.K. commanding officer had "full visibility of the US [standard operating] procedures" for the handling of detainees, which the officer's team determined fell within the requirements of the Geneva Conventions.[187] The U.K. ISC Rendition and ISC Detention Reports reflect various instances in which U.K. officers were authorized to try to stop interrogations, were required to express concerns to U.S. officials about any abuse

---

[182] *See, e.g.*, ISC Detention Report, *supra* note 90, at ¶ 47 (releasing information sent from London to U.K. intelligence officers in Afghanistan regarding U.S. ill-treatment of detainees).

[183] Ryan Goodman, *UK Detainee Inquiry Report Details Britain's Involvement in US Torture and Rendition Programs*, JUST SECURITY (Dec. 19, 2013), https://www.justsecurity.org/4842/uk-detainee-inquiry-report-exceprts/.

[184] SENATE SELECT COMM. ON INTELLIGENCE, COMM. STUDY OF THE CENT. INTELLIGENCE AGENCY'S DETENTION AND INTERROGATION PROGRAM, S. REP. NO. 113-288, at v–vi (2014) (noting that report reveals "significant amount" of new information); *id.* at 14 n.28 (mentioning foreign detention sites, though not by country name); GOLDSMITH, *supra* note 1, at 213; Radu-Sorin Marinas & Christian Lowe, *U.S. Torture Report Puts Romania's Role Under Scrutiny*, REUTERS (Dec. 17, 2014), http://www.reuters.com/article/2014/12/16/us-usa-cia-torture-romania-idUSKBN0JU29H20141216 (noting that the SSCI Report has shone an uncomfortable light on some European states that hosted secret detention facilities).

[185] Silvia Borelli, *Rendition, Torture and Cooperation*, *in* INTERNATIONAL INTELLIGENCE COOPERATION, *supra* note 9, at 107.

[186] ISC Detention Report, *supra* note 90, at ¶ 95.

[187] *Id.*

they saw, and intervened with their U.S. peers. The ISC Detention Report illustrates one such instance, quoting instructions to U.K. personnel:

> HMG's stated commitment to human rights makes it important that the Americans understand that we cannot be party to such ill treatment nor can we be seen to condone it. In no case should they be coerced during or in conjunction with an SIS interview of them. If circumstances allow, you should consider drawing this to the attention of a suitably senior US official locally.[188]

If an SIS officer in the field witnessed problematic interrogation techniques used during detainee interviews, that SIS officer was under instructions to ask the state interviewing the detainee to stop the interview, state his concerns, withdraw from the interview, and report the incident to his head office.[189] The United Kingdom subsequently reported that it had followed up with the United States on most of the incidents of mistreatment described in the ISC Detention Report, "either in theater or through intelligence and diplomatic channels."[190]

Some of these on-the-ground interactions altered—that is, constrained—how the United States treated detainees. In June 2003, a U.K. officer who had been present while the United States interviewed a detainee noted that the detainee expressed concern about lack of family contact.[191] The U.K. official raised the concern with the United States and was able to arrange for the detainee to contact his family. One month later, a different detainee expressed similar concern to a U.K. IC official about lack of family and ICRC access; SIS arranged to have him contact his family by phone.[192]

These rights-protective outcomes arise because the peer imposes transaction costs on the state that is conducting a particular operation. For example, if an IC official from one state observes one of his counterparts acting in a way that deviates from the agreed constraint, the first official has the opportunity (and sometimes the responsibility as a matter of law or policy) to bring the deviation to his counterpart's attention. Indeed, U.K. IC officials are instructed to make themselves aware of the U.K. government's views on the legal framework and practices of the liaison services with which they interact. Thus, if a U.K. official is the peer observer, he is likely to know something about the legal

---

[188] *Id.* at ¶ 47.
[189] U.K. Detainee Inquiry, *supra* note 46, at 5.59; *id.* at 5.44 (noting that SIS officers were instructed to pass to U.S. authorities any detainee complaints of mistreatment and, if SIS officers witnessed mistreatment, to register their concern with U.S. authorities at the earliest opportunity).
[190] GOVERNMENT RESPONSE TO THE INTELLIGENCE AND SECURITY COMMITTEE'S REPORT ON THE HANDLING OF DETAINEES BY UK INTELLIGENCE PERSONNEL IN AFGHANISTAN, GUANTANAMO BAY AND IRAQ, 2005, Cm. 6511, at 3 (U.K.).
[191] ISC Detention Report, *supra* note 90, at ¶ 87.
[192] *Id.* at ¶ 90.

rules with which his peer IC counterpart should be complying.[193] Even if the counterpart continues to deviate, the actions of the peer (and sometimes the peer's mere presence) have imposed transaction costs on the counterpart by forcing him to explain and defend his action. Further, psychologists have shown that people behave differently when they know they are being watched.[194] Consequently, the presence of peer IC officials during actual operations may constrain the behavior of a given IC, either directly (as when the peer IC official intervenes in an interrogation) or indirectly (as when the mere presence of a peer official affects the way the given IC chooses to behave).

C. *Naming and Shaming*

A third mechanism by which a state can constrain a partner IC is through the use of overt political pressure, as when State X publicly criticizes State Y for engaging in particular intelligence activities that have come to the attention of State X's officials. The actors issuing such critiques have invoked different principles of domestic and international law, based both on the factual scenario being criticized (Did the surveillance take place from within an embassy? Did the IC being criticized engage in a covert action that employed coercive action against an individual overseas?) and on the particular critiquing state's understanding of the applicable law (Did the embassy-based surveillance violate the Vienna Convention on Diplomatic Relations? Did the IC undertaking a forcible covert action have a legitimate self-defense justification, or did its act violate the U.N. Charter?). When these criticisms produce changes to a peer IC's policies, they serve as peer constraints. Although naming and shaming has long been understood as a mechanism by which states can influence each other's behavior,[195] only recently have states undertaken extensive naming and shaming in the spying context. This mechanism may involve different actors from those in other mechanisms discussed in this article, but we may nevertheless consider senior officials to be part of an intelligence community as long as they play a role in setting intelligence policy or regulating IC activities.[196]

---

[193] U.K. Detainee Inquiry, *supra* note 46, at 5.95.

[194] Deeks, *supra* note 156, at 830 (citing psychological phenomenon in which people modify their behavior when they know someone is studying them). It is clear that U.K. officials were "watching" U.S. detention operations, though it is not clear whether the United States knew the U.K. officials were recording the terms under which U.S. officials were conducting interviews and making other "pertinent observation[s] about the American detention regime" that they would send back to the Foreign and Commonwealth Office and the Home Office. U.K. Detainee Inquiry, *supra* note 46, at 5.35–36. The more that U.S. officials were aware of the U.K. reporting, the stronger the psychological effect would have been.

[195] *See generally* RYAN GOODMAN & DEREK JINKS, SOCIALIZING STATES: PROMOTING HUMAN RIGHTS THROUGH INTERNATIONAL LAW (2012); Emilie M. Hafner-Burton, *Sticks and Stones: Naming and Shaming the Human Rights Enforcement Problem*, 62 INT'L ORG. 689 (2008).

[196] For ease of discussion, this article also treats many of the decisions setting intelligence policy as emerging from a state's IC, rather than a state more generally. But often the laws and policies that regulate a state's IC emerge from more senior actors within a state, such as the President or

As a recent example, the Snowden leaks about U.S. and U.K. foreign electronic surveillance—including allegations that the NSA was spying on the senior leadership of U.S. allies—produced high levels of criticism by peer states such as Germany, Brazil, and Mexico.[197] German Chancellor Angela Merkel angrily chastised President Obama for allowing the United States to listen to her phone calls.[198] Similarly, Brazilian President Dilma Rousseff cancelled her state visit with President Obama to send a clear signal of Brazil's displeasure that the NSA was tapping her calls.[199]

These critiques helped compel a change in U.S. policy. In a January 2014 speech, President Obama announced, "[U]nless there is a compelling national security purpose, we will not monitor the communications of heads of state and government of our close friends and allies."[200] Also in January 2014, the Obama Administration released Presidential Policy Directive 28 on Signals Intelligence Activities, which suggests that the United States will limit its existing surveillance of certain states' leadership and engage in more careful consideration before initiating collection on the leadership of a significant number of states.[201] The AP subsequently reported that the CIA had "curbed spying on friendly governments in Western Europe in response to the furor over a German caught selling secrets to the United States and the Edward Snowden revelations of classified information held by the National Security Agency."[202] If that report is accurate, the U.S. policy decision to suspend collection is an example of a peer constraint flowing in notable part from public naming and shaming.

Although naming and shaming is intended to constrain the behavior of other states, some of the naming and shaming has the unexpected effect of producing *self-constraints* on the states that are critiquing other ICs. Consider the critiques levied against the types of electronic surveillance conducted by the NSA

Prime Minister, or from parliaments. Thus, the IC executes intelligence policies but may not always set them.

[197] Der Spiegel Staff, *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, DER SPIEGEL (Oct. 27, 2013), http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (describing spying out of U.S. Embassy in Berlin); Jens Glusing, Laura Poitras, Marcel Rosenbach & Holger Stark, *NSA Accessed Mexican President's Email*, DER SPIEGEL (Oct. 20, 2013), http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html (describing spying out of U.S. Embassies in Mexico City and Brasilia).

[198] Geir Moulson & John-Thor Dahlburg, *Angela Merkel's Cell Phone Tapped by NSA? U.S. Accused of Spying on German Chancellor*, HUFF. POST (Oct. 23, 2013), http://www.huffingtonpost.com/2013/10/23/merkel-phone-tapped_n_4150812.html.

[199] Glusing et al., *supra* note 197.

[200] Obama NSA Speech, *supra* note 79.

[201] White House Office of Press Sec'y, *Presidential Policy Directive: Signals Intelligence Activities*, § 3 (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (stating that it is "essential that national security policymakers consider carefully the value of signals intelligence activities in light of the risks entailed in conducting these activities").

[202] Ken Dilanian, *CIA Halts Spying in Europe*, ASSOCIATED PRESS (Sept. 20, 2014).

and GCHQ. States ranging from Germany to Indonesia to the Bahamas have argued that the United States and United Kingdom are engaged in international law violations, including violations of sovereignty and the right to privacy.[203] By taking these positions publicly, these states make it harder for themselves to claim that their own foreign surveillance activities are consistent with international law. To be sure, it is possible to argue that particular types of surveillance (such as that which does not take place against diplomatic missions or assemble internet or telephony content in bulk) will not implicate international legal principles. But the more states make affirmative statements about the illegality of particular kinds of espionage, the more they constrain their own ICs, or at least their own ability to claim that those actions are lawful.[204] Naming and shaming therefore can serve both as a form of peer constraint and a form of self-constraint on ICs.

*****

These three manifestations of peer constraints—formal constraints, informal constraints (driven both by black letter domestic laws and perceptions of future legal requirements and oversight), and naming and shaming—all serve to influence the behavior of ICs that partner with other ICs. Having identified how the mechanisms operate, it is important to try to assess how robust those mechanisms are and what advantages they may offer—if any—over other, more visible IC oversight mechanisms. It is also necessary to consider whether the mechanisms described herein more often function as tools to facilitate IC abuses of individual rights rather than limit such abuses. The following Part undertakes these analyses.

IV. Evaluating Peer Constraints

A. *Conceptual Advantages of Peer Constraints*

Peer constraints offer at least four advantages that are not found in oversight stemming from bodies such as parliamentary intelligence committees, inspectors general, or independent, executive-created bodies.[205]

---

[203] Deutsche Welle, *supra* note 95 (Germany); Miller, *supra* note 95 (Germany); U.N. Press Release, *supra* note 96 (Indonesia); Rashad Rolle, *Lawyers to Act in N.S.A. Spy Row*, TRIBUNE 242 (June 5, 2014), http://www.tribune242.com/news/2014/jun/05/lawyers-act-ns-spy-row/ (Bahamas).

[204] For example, various commentators condemned Germany for hypocrisy when the media revealed that Germany had been cooperating with the NSA in spying on European (including German) companies. Henry Farrell, *The New German Spying Scandal is a Big Deal*, WASH. POST: MONKEY CAGE (Apr. 23, 2015), https://www.washingtonpost.com/blogs/monkey-cage/wp/2015/04/23/the-new-german-spying-scandal-is-a-big-deal/.

[205] Some forms of peer constraints work in part because of the existence and work of these other oversight bodies, so I do not mean to suggest that peer constraints should serve as a replacement for any of these other bodies.

First, peer ICs can understand the technologies and techniques of other ICs in ways that those other bodies cannot. This is not to suggest that those outside the IC cannot gain a sophisticated understanding of how intelligence operations work. However, no other actor is better suited to grasp the nuance of intelligence requirements, tools, and tradecraft than a peer IC. It is difficult for Congressional committees, courts, and civil liberties groups to understand (or have access to) the complicated technology of ICs, which erects certain hurdles to true oversight.[206] As Amy Zegart explains, one reason that Congressional oversight in the United States has proven weak is that "intelligence is a highly technical and cloistered business, requiring years of study or insider experience to understand."[207] To this extent, partner ICs are in a better position to understand intelligence operations and to flag—at least in some cases—legal or compliance problems.[208] As the U.K. ISC puts it, "The [U.K.] Agencies' knowledge of the workings of foreign liaison services is critical in assessing the risks involved in cooperation with them."[209] That knowledge is relevant not only for assessing the liaison IC's own legal risks, but also for engaging in dialogue with peer ICs about their legal and policy compliance.

Second, as discussed in Part III, peer ICs engaged in joint operations are in a better position than any other oversight body to directly observe the activities of their partner ICs. Oversight bodies such as SSCI can evaluate intelligence programs *ex ante* and, along with entities such as courts and the U.S. Privacy and Civil Liberties Oversight Board (PCLOB), can evaluate those programs *ex post* as well. But they do so at a temporal and geographic remove. There is something distinct and particularly salient about a role for a "watcher" in a given operation. Knowledge by the IC that it ultimately will have to face hard questions from Congress affects the way in which the IC shapes a given operation.[210] But knowing that one or more peer ICs will be aware of the specifics of an operation and possibly will participate in it will affect both how one IC thinks in advance about how to conduct that operation and, in cases in which the planning IC believes that it is operating in a gray area, may cause it to tighten up the rules it sets for itself and the way in which the operation actually plays out.

Third, liaison partners can offer particular kinds of carrots and sticks that other oversight bodies cannot. While congressional overseers have the power of

---

[206] Even the White House may lack (by choice or capacity) full visibility into and control over the volume of IC decisions and information. *See* Aziz Huq, *Structural Constitutionalism as Counter-terrorism*, 100 CALIF. L. REV. 887, 914 (2012).

[207] Amy B. Zegart, *The Roots of Weak Congressional Intelligence Oversight*, HOOVER INSTIT. (2011) at 6. *See also id.* at 10 (noting that Congressional oversight requires delving into "highly technical issues without watchdog groups or any other information sources freely available in the unclassified world.").

[208] *See* Sepper, *supra* note 4, at 191 ("Intelligence professionals are those most likely to become aware of impropriety by partner agents and are therefore the best actors to conduct oversight and demand compliance with professional guidelines.").

[209] ISC Rendition Report, *supra* note 84, at ¶ 175.

[210] GOLDSMITH, *supra* note 1, at 92.

the purse, it is often politically challenging to cut an intelligence service's budget.[211] Other actors such as executive branch prosecutors undoubtedly carry serious sticks in the form of the ability to conduct criminal investigations and file charges against IC officials who violate the law, but those prosecutions are infrequent. Entities such as the PCLOB, civil liberties groups, and the media have the power of persuasion, but often have little to wield by way of sticks.[212] The fact that partner ICs—at least in some circumstances—have more direct carrots (in the form of intelligence to share or permission to give to operate on their territory or in their airspace) and sticks (in the form of intelligence to withhold or denial of such permission) may make their influence as persuasive to their peers as those overseers who have only sticks (and relatively modest or indirect ones at that). Peer ICs can also monitor and follow through on the on-the-ground commitments of another IC in a way that overseers further removed from operations cannot.[213]

Finally, peer constraints are relatively de-politicized because there usually will be no public audience for the constraining act. Peer constraints usually happen behind a veil of secrecy. Whereas overt oversight of ICs may be infused with politics, it is difficult to use peer constraints (other than naming and shaming) to achieve overt political goals because the public rarely will know that the liaison interaction even took place. Opacity of IC activity, therefore, has an upside: peer constraints avoid critiques made only for political gain. In both formal and informal constraining contexts, a state applies a constraint on a peer IC not to "be seen" complying with legal rules but actually to comply with legal rules—at least as interpreted by the executive branches of those states. Compare the process Goldsmith describes: members of Congress are reluctant to put themselves on record as approving or critiquing particular intelligence activities.[214] As a result, they engage only cursorily, and then, when an issue becomes public and controversial, distance themselves from it. Only then do members of Congress conduct true oversight.[215] Politics play a greatly diminished role in the formal and informal peer constraints discussed in Part III.

B. *Strength of the Constraints*

The earlier Parts of this article argued that peer constraints exist among ICs and analyzed the different forms those constraints can take. In light of the fact

---

[211] Zegart, *supra* note 207, at 13, 15 (describing limited leverage of intelligence authorizers and ways in which IC circumvents authorizers to secure appropriations).

[212] *See* Aldrich, *supra* note 9, at 35 (describing lack of power of European Parliament and Commission to secure responses from national governments on their rendition and secret detention sites reports).

[213] *See, e.g.*, Arar Report, *supra* note 109, at 347 (calling for Canadian IC to monitor the use of information by the liaison partner that received it from Canada). Canada implemented twenty-two of the twenty-three Arar Report recommendations, presumably including this one.

[214] GOLDSMITH, *supra* note 1, at 92.

[215] Huq, *supra* note 205, at 926–27 (noting limited incentives of members of Congress to spend time overseeing counter-terrorism activity).

that most intelligence activity remains classified and inaccessible to the public, however, can we know how strong the constraints actually are? Although it is very difficult to say with certainty how effectively the constraints operate in any particular situation, it is possible to reach some tentative conclusions about when peer constraints will be stronger or weaker. Constraints are likely to be stronger when the ICs cooperating with each other are from states that are committed to the rule of law; when they are cooperating on an issue that is of key importance to the state being constrained; and when the constrained IC cares about its reputation among its peer ICs.

1. Commitment to the rule of law

The extent to which a particular IC is committed to the rule of law and/or is heavily regulated by law plays a significant role in the level of constraint that the IC will impose on others. Assume that the ICs of rule-of-law states (ROLS) are under significant legal regulation and generally have a culture of compliance with those regulations. The ICs of non-rule-of-law states face lighter or no regulation and adhere to laws less consistently.

Peer constraints will tend to be stronger among ROLS, which generally are committed to diligent compliance with domestic legal requirements. ROLS are more likely to impose peer constraints on others, and are more likely to respect the fact that other states may need to impose constraints on them. This means that the level of legalization of an IC in a ROLS and the quantum of oversight that IC faces will have a direct impact on the amount of constraint that IC will need to impose on its liaison partners. This also suggests that the trends of increased legalization of intelligence issues and the concomitant acceptance (whether grudging or embracing) of this legalization among ICs in ROLSs mean the possibility of peer constraints will only grow. And as it becomes harder and harder to keep secret IC activities secret, ICs and their senior executive branch decision-makers are more likely to impose rigorous policy constraints on themselves for fear of backlash if their activities are disclosed—a process that only serves to add to the pile of constraints already in play. In short, there are a limited number of states today that likely need to constrain their liaison partners, but the imperatives of constraint are on the rise as those constraining ICs face increased domestic legal regulation. There are a greater number of ICs on the "constrained" side of the equation, either because those ICs have questionable human rights records or because they simply lack domestic regulation.

2. Importance of the cooperation

We also can predict that constraints will be stronger when the state facing a peer's constraint firmly desires the intelligence or IC cooperation that the peer is offering. Such a desire is affected by how many alternatives the assistance-seeking IC has: if the constraining peer stands as the best (or only) source of a particular piece of intelligence, or if the peer has the only airport or territory that will allow the constrained state to conduct a particular operation, the latter is more

likely to accede to the constraint. Yet if an IC (whether a ROLS or not) has a variety of options to achieve a particular goal, it may use the less constraining alternative, assuming the alternative would not run afoul of its own domestic legal constraints. In short, the size and uniqueness of the carrot being offered by the constraining state has a direct effect on whether the recipient state will accept the constraint.[216]

As a related matter, how quickly a state needs cooperation will affect the level of constraints it is willing to accept. If a state requires immediate assistance from another state, the requested state has significant leverage to impose constraints if it chooses to. If the state has ample time to develop sources of intelligence and forms of cooperation from states that are unlikely to impose constraints on it, it is likely to pursue this latter route. For instance, if France learns that a high-level terrorist it was tracking has had repeated cell phone conversations with a co-conspirator in Australia and has boarded an airplane flying from France to Australia, France will urgently desire cooperation from Australia's IC. Australia is by far the state best positioned to help France and, given the urgency with which France desires assistance, France will likely agree to a wide set of constraints that Australia may wish or need to impose on its cooperation with France.

3. Reputational concerns

Third, in cases in which constraints manifest themselves as critiques of a peer IC's actions (whether during an interrogation on the ground or in a name-and-shame context), those constraints will have more bite when the IC on the receiving end of the critique cares about its reputation in the eyes of the peer. It might care because it often needs assistance from this peer and thinks it will be able to procure this assistance only if the peer sees it as law-abiding. Or it might care for less instrumental reasons: perhaps it wants to see itself as a reliable and law-abiding ally. A useful analog here is "acculturation," a theory that Ryan Goodman and Derek Jinks use to explain how states influence the behavior of other states.[217] Their theory, which stands in some contrast to two other explanations for why states comply with international norms (that is, coercion and persuasion), captures "the general process by which actors adopt the beliefs and behavioral patterns of the surrounding culture. This mechanism induces behavioral changes through pressures to assimilate—some imposed by other actors and some imposed by the self."[218] Conformity with norms follows from the

[216] For those seeking to magnify the operation and effect of peer constraints (as NGOs might), this suggests that there are certain states that may serve as linchpins, either because they are located in strategically important areas or because they have unique access to particular information. Those who wish to magnify peer constraints will urge those linchpin states to enact rights-protective laws that apply to their ICs.

[217] Ryan Goodman & Derek Jinks, *How to Influence States: Socialization and Human Rights Law*, 54 DUKE L.J. 621 (2004).

[218] *Id*. at 626.

pressure of others who are within the same "group." As Goodman and Jinks put it, "The touchstone of this mechanism is that identification with a reference group generates varying degrees of cognitive and social pressures—real or imagined—to conform."[219] When President Obama remarked in January 2014, "For our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world,"[220] his statement reflected a certain amount of acculturation to the idea that states should restrain their surveillance of foreign nationals.

The likelihood of conformity with norms for reputational reasons turns on the importance of the group to the target actor, the amount of exposure an actor has to the relevant group, and the size of group (where smaller groups create more potent compliance).[221] As Goodman and Jinks state,"[S]mall group size promotes acculturation because small groups are more likely to foster intimate, high-affect exchanges. Regimes with restricted membership, therefore, should facilitate the convergence of practices." [222] ICs collectively have developed a particular professional culture that emphasizes the need to act objectively and in pursuit of truth.[223] Elizabeth Sepper has noted that acculturation may operate within IC networks to produce strong incentives to comply with those professional standards. [224] While Sepper is skeptical that acculturation produces rights-enhancing outcomes, she ignores the fact that the professional standards to which states are acculturating may (and now in many cases do) incorporate legal compliance as part of the body of norms.[225] Thus, when an IC is susceptible to acculturation—as many ICs in democracies and ROLSs likely are—the imposition of peer constraints is likely to be more effective.

As this discussion shows, peer constraints can play an important and unique role in modulating the activities of other ICs, but are hardly a replacement for other forms of IC oversight. Instead, peer constraints supplement and in many ways rely on oversight from other sources, while bringing to the table certain unique advantages that other actors interfacing with ICs lack.

C. *Critiques*

The argument that peer constraints exist and can have a rights-protective influence on the operations of other ICs is open to several challenges. One might question, for instance, how frequently peer constraints operate, or how effectively peer constraints work on states that rarely require cooperation because they have

---

[219] *Id.*
[220] Obama NSA Speech, *supra* note 79.
[221] Goodman & Jinks, *supra* note 217, at 642.
[222] *Id.* at 672.
[223] Sepper, *supra* note 4, at 159.
[224] *Id.* at 163.
[225] Sepper argues that ICs constrain each other based "almost exclusively" on shared professional ethos rather than law. *Id.* at 151.

robust intelligence capabilities of their own. This section considers those critiques and others.

1. Limited number of constraining ICs

Even if certain ICs can and do impose peer restraints on other ICs, one possible critique is that the number of constraining ICs is small. The bulk of the constraining ICs is likely to be western democracies that have functional judicial and parliamentary systems, a tradition of legal compliance, a robust media, and a susceptibility to public pressure and critiques—that is, ROLSs.[226] This fact does not undercut the idea that peer constraints exist; it only means that a finite number of ICs are likely to act as constraining states in their relationships with liaisons. Importantly, the bulk of those states that fall within the constraining state category are states with extensive intelligence capacities. This means they have intelligence and capabilities from which other states would like to benefit. As a result, the constraints are more likely to have teeth. That said, when none of the ICs cooperating in a particular situation faces legal constraints on its activities, there will be no peer constraints in evidence.

2. Non-binding nature of constraints

Another critique is that, unlike treaties, peer constraints often are not legally binding. As a result, a constraining state generally will have a difficult time enforcing the constraints as a legal matter. Additionally, many constraints come in unwritten form, which can foster disagreement about the substance of the constraint or questions about interpretation. The somewhat lower transaction costs that arise in oral agreements suggest that the agreements may be altered relatively easily. Finally, some of the constraints being imposed by one IC on another may be based on policy decisions rather than legal requirements. This suggests that the constraints may be more negotiable because they represent policy positions rather than matters of binding domestic law.

It is true that peer constraints almost always will be less obviously enforceable than public bilateral or multilateral treaties. The arrangements are enforceable diplomatically or politically, however, and when peer ICs are repeat players, that type of enforcement carries real weight. Debates about the meaning of particular agreements are common, even when agreements are public and in writing. Moreover, the fact that some constraints (such as those developed in the shadow of the observer effect, or out of concern about public disclosures by oversight bodies) are driven by legal policy concerns rather than black letter law does not render them infinitely flexible. Rather, legal policy concerns can be as potent as purely legal concerns in the area of intelligence, and states with those concerns are likely to enforce both types of constraints.

[226] It is hard to imagine, for instance, that China requires treatment assurances before sharing information with a partner IC that would allow the partner to locate and detain an individual.

3. Sacrifice of principles for security

Those who emphasize the insular and hidden nature of ICs will point to cases in which even ROLSs such as the United States have chosen to engage in activity that violates international law and norms—sometimes egregiously. The recent release of the SSCI Report discloses both treatment of detainees that most of the international community would describe as torture and liaison cooperation that facilitated—rather than constrained—that detention and treatment. States that fear terrorist attacks and are under pressure to take robust measures to defeat those threats often make decisions and take actions that prove harsh, foolhardy, or counter-productive in hindsight. These decisions can take at least four forms.

First, states may decide to overtly break the law.[227] A state that has made this decision will neither constrain other ICs nor respond to peer IC constraints. Second, one IC might seize opportunities to circumvent its own laws by relying on other states to achieve for it what it cannot, or by taking advantage of situations created by liaison cooperation. For example, the Washington Post reported that Alliance Base allowed German intelligence officers to read German law enforcement information, something German intelligence cannot do directly within Germany.[228] Third, if an IC assumes that its operations will remain secret, it may choose to pressure a peer IC to operate at the outer limits of the latter's legality, rather than attempt to constrain the peer or encourage the peer to operate well within the bounds of the peer's domestic laws.[229] Fourth, the fact that ICs generally operate in secret may create disincentives for any one IC to call to account its partners, particularly where those partners provide it with critical intelligence.[230] If the partners' actions are unlikely to come to light, the cost of criticizing or constraining the partners may appear higher than any benefit to be achieved by insisting on "secret" legal compliance. One can find various

[227] This seems to be the case with some CIA employees who used unapproved interrogation techniques. S. REP. NO. 113-288, at xxi (noting that some detainees were subject to techniques that were not legally authorized). The U.K. Foreign Secretary gestured at the tensions that occasionally may arise between legal compliance and security when he stated, "[M]y last point is a real area of moral hazard . . . . [If] you do get a bit of information which seems to be completely credible, but which may have been extracted through unacceptable practices, do you ignore it? And my answer to that is . . . you have to make an assessment about its credibility. . . . [Y]ou cannot ignore it if the price of ignoring it is 3,000 people dead." ISC Detention Report, *supra* note 90, at ¶ 33.

[228] Priest, *supra* note 31. *See also* S. REP. NO. 113-288, at ix (noting that CIA chose to detain Abu Zubaydah not at a U.S. military facility, where CIA would have had to declare him to the International Committee of the Red Cross, but at a secret site in a different country).

[229] S. REP. NO. 113-288, at xxii (stating that CIA asked host states to hold some detainees who did not meet the legal standards for U.S. detention, even though host states had no independent reason to hold the individuals); Sepper, *supra* note 4 (arguing that intelligence liaison networks systematically have undermined human rights treaties).

[230] For instance, the U.K. Detainee Inquiry raised questions about whether the U.K. IC surfaced with sufficient vigor allegations of mistreatment of detainees with liaison partners, and about whether the assurances the U.K. sought were adequate. U.K. Detainee Inquiry, *supra* note 46, at 7.6.

examples in the post-September 11 years where the United States stopped criticizing partner states for their human rights records to encourage intelligence cooperation by those partners.[231]

Some of these critiques are more potent than others. With regard to the concern about relying on peer ICs to circumvent one's own domestic constraints, many of the ICs discussed here are bound by policies or laws that forbid them from asking other ICs to pursue actions they themselves could not undertake. In the United States, Executive Order 12,333 states, "No element of the Intelligence Community shall participate in or request any person to undertake activities forbidden by this order."[232] The NSA recently confirmed this policy, stating that the agency "does not ask its foreign partners to undertake any intelligence activity that the US government would be legally prohibited from undertaking itself."[233] Likewise, Canada has denied that it uses peer services to obtain information about Canadian citizens indirectly that it could not lawfully collect directly.[234] The U.K.'s ISC recently concluded that GCHQ did not circumvent U.K. law by using a NSA program to obtain the contents of private communications.[235] And states that are subject to ECtHR jurisprudence have long been bound by the *Soering* doctrine. Under the logic of that case, a state may not create a "real risk" that a person will be exposed to treatment that would violate the ECHR. That rule precludes transfers to another state that might engage in treatment that would violate the ECHR, even if the receiving state is not a party to the ECHR.[236]

---

[231] Priest, *supra* note 17 (describing CIA assistance to states with problematic human rights records, including Uzbekistan and Indonesia); Scott Shane, *CIA Role in Visit of Sudan Intelligence Chief Causes Dispute Within Administration*, N.Y. TIMES (June 18, 2005), http://www.nytimes.com/2005/06/18/politics/cia-role-in-visit-of-sudan-intelligence-chief-causes-dispute-within-administration.html (noting controversy of inviting Sudan's intelligence chief to Washington in light of allegations that Sudanese government was engaged in genocide and had terrorist ties).

[232] Exec. Order No. 12,333, *supra* note 111, at sec. 2.12.

[233] Ackerman & Ball, *supra* note 38; *see also* Rosalba O'Brien & Michael Holden, *British spy agency taps cables, shares with U.S. NSA*, REUTERS (June 21, 2013), http://www.reuters.com/article/2013/06/21/usa-security-britain-idUSL5N0EX39I20130621#lUHVRcTGE6rrkftC.97 ("'Any allegation that NSA relies on its foreign partners to circumvent U.S. law is absolutely false. NSA does not ask its foreign partners to undertake any intelligence activity that the U.S. government would be legally prohibited from undertaking itself,' [NSA Spokeswoman Judith] Emmel said.").

[234] CSIS officials indicated that it would be inappropriate for CSIS to ask the U.S. government to intercept a particular Canadian communication as it passed through the United States in an effort to circumvent Canadian privacy laws. "Such behavior would draw the attention, and likely ire, of CSIS's review institutions: the inspector-general and the Security Intelligence Review Committee." Craig Forcese, *The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights of Transnational Intelligence Sharing*, *in* INTERNATIONAL INTELLIGENCE COOPERATION, *supra* note 9, at 80, 82.

[235] Statement by the Intelligence and Security Commission of Parliament, ISC Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme (July 17, 2013), http://isc.independent.gov.uk/news-archive/17july2013.

[236] Soering, *supra* note 149.

The critique that ICs often have limited incentives to challenge each other's compliance with the law (or policy, or morality) is a fair one. For example, European states whose nationals have traveled to Syria to fight may be relying on U.S. intelligence even if they have some misgivings about certain U.S. IC activities.[237] But the potency of this critique appears to be fading in view of the clear sense among ICs that it is very difficult to keep secret activities secret for any extended period of time. Thus, not only will troubling acts be made public, but the cooperation of peer ICs in those acts will also be made public. This significantly increases the incentives of at least some ICs to challenge and constrain.

There clearly are situations in which ICs do not constrain each other. The goal of this article is not to argue that peer ICs operate in all situations, or that they serve as a potent stand-alone tool for modulating IC behavior. Rather, the goal is to demonstrate that peer IC constraints exist and to explore how and why they function. Further, there is reason to believe that peer constraints will become a more common and robust phenomenon as leaks, litigation, and IC legalism continue to proliferate. As legal strictures become increasingly infused in the culture of certain groups of ICs, the phenomenon of acculturation may spread that culture to other IC partners. Peer constraints can produce highest common denominator behavior, but they do not always operate. Institutions make mistakes, and ICs are no exception. The fact that ICs have engaged in abuses and controversial activities does not undercut the fact that there are cases in which peer ICs pull in the opposite direction, toward a more cautious and rights-protective approach to liaison relationships. Indeed, controversial actions can create a backlash that end up amplifying both the laws and oversight activities of ICs,[238] opening the door for a cyclical amplification of peer constraints.

4. Tying Gulliver down?

Skeptics will argue that it is nearly impossible to constrain the IC of a superpower—in this case, the United States. On this theory, if one state has significantly greater intelligence capabilities than other states, the likelihood that that state will need assistance from any particular peer liaison service is quite small. The Gulliver IC may be able to obtain the desired assistance from another service that does not intend to impose constraints, or it may be able to undertake the desired action (arresting an individual, say) itself, even if it would be easier or more appealing to have another state arrest the person for it. As a result, the superpower rarely will find itself in a situation in which it needs to accept peer constraints in order to achieve its intelligence goals.

---

[237] Greg Miller, *Backlash in Berlin over NSA Spying Recedes as Threat from Islamic State Rises*, WASH. POST (Dec. 29, 2014), https://www.washingtonpost.com/world/national-security/backlash-in-berlin-over-nsa-recedes-as-islamic-state-rises/2014/12/29/c738af28-8aad-11e4-a085-34e9b9f09a58_story.html.

[238] GOLDSMITH, *supra* note 1, at 250–51.

Without a doubt, there are cases in which one state refuses to be constrained by another. For example, the United Kingdom became concerned that the United States was using a U.K. base in Cyprus to launch intelligence-gathering flights that obtained information about the location of Hezbollah militants.[239] The United Kingdom worried that the United States was passing that information to Lebanese authorities who might mistreat those militants in detention. Notwithstanding repeated demands from the United Kingdom that the U.S. Embassy provide full details of its flights so that the United Kingdom could assess whether it was "at risk of being complicit in unlawful acts," the United States refused to do so.[240] To some extent, this case is not typical, in that the role of the U.K. IC in the operations was quite tangential. Yet it illustrates the level of concern about legal exposure within the U.K. government as well as the fact that peer constraints are not always effective, particularly where the state that would otherwise be constrained may believe that the constraining state is taking an unduly legalistic or cautious approach to its own legal framework.

One answer to this critique is that even Gulliver needs assistance, at least periodically.[241] Sometimes the Gulliver state has no choice but to work with a particular IC. Perhaps the person the Gulliver IC is seeking is in the custody of State X or perhaps the electronic communications that the superpower requires can only be decrypted by State Y. Maybe the Gulliver state desires information from one or more peers that can corroborate (or call into question) the intelligence Gulliver already has. One can imagine a number of situations in which liaison cooperation is not optional. It still may be the case that the less powerful IC chooses not to constrain the superpower IC in any meaningful way, perhaps because the less powerful IC views the costs of doing so as too high. But for peer ICs that have longstanding and durable relationships with the superpower and sufficiently valuable intelligence to offer over time, the superpower IC will realize that, as a repeat player, accepting certain constraints may be in its longer-term interest.

Recent developments show that even the U.S. Gulliver ultimately can be tied down in some areas by "Lilliputian" states.[242] The U.S. detention and interrogation program offers an example. As the SSCI Report notes, "With the exception of [one country], the CIA was forced to relocate detainees out of every

---

[239] Richard Norton-Taylor & David Leigh, *UK overrules on Lebanon spy flights from Cyprus, Wikileaks cables reveal*, THE GUARDIAN (Dec. 1, 2010), http://www.theguardian.com/world/2010/dec/01/wikileaks-cables-cyprus-rendition-torture.

[240] *Id.* It is unknown whether the U.K. continued to allow the United States to fly from its Cyprus base after the United States refused to share flight information.

[241] *See supra* Part I.A.

[242] Peer constraints against a superpower are likely to vary in their efficacy depending on what acts the constrainers seek to constrain. In view of the ever-expanding (and arguably legitimate) interest in gathering information and the powerful capacity of the United States to collect that information electronically, constraints are unlikely to have a robust effect on that collection. Constraints are more likely to operate as a check on outright abuse or on certain uses of information or assistance (even if not clear abuses of authority).

country in which it established a detention facility because of pressure from the host government or public revelations about the program."[243] By 2006, the CIA concluded that it was "stymied" and the "program [of secret detention and interrogation] could collapse of its own weight."[244] Shortly thereafter, the United States shut those secret facilities. If globalized trends related to national security threats continue to abound, there will continue to be many cases in which no single IC can manage those threats on its own.

Conclusion

NSA's spokeswoman recently stated, "NSA works with a number of partners in meeting its foreign-intelligence mission goals, and those operations comply with U.S. law and with the applicable laws under which those partners operate."[245] In other words, NSA and its partners are peer-constrained. More broadly, the ICs of various states are forced to respond to domestic legal limitations imposed by their counterparts. Peer constraints offer an underexplored way in which ICs modify their behavior based on legal rules.

Scholars, government actors, and citizens who seek to ensure the existence of a variety of effective oversight mechanisms must keep in mind the little-noticed but important role that peer constraints can play in protecting individual rights. States that are committed to the rule of law should take advantage of the opportunities that peer constraints create. Those states, which often will serve as "constraining" states, should consider how they might use their intelligence relationships to improve the practices of states that are less committed to the rule of law and to humane treatment of people in their custody. Their ICs are well suited to help persuade non-rule of law states that certain rights-protective laws can contribute to, rather than detract from, the efficacy of intelligence activities. Diplomats and non-governmental organizations are not the only actors in the international arena who can do this; indeed, ICs may be best placed to persuasively deliver this message to their peers.

The direction in which leaks, litigation, and legalization are trending indicates that these constraints are only likely to grow in strength and complexity. Understanding when and how peer constraints operate will allow states to take advantage of the mechanism to affect their counterparts' activities in years to come.

---

[243] S. REP. NO. 113-288, at xxiv.
[244] *Id.*
[245] James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES (Feb. 15, 2014), http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html.