American University National Security Law Brief

Volume 9 | Issue 1 Article 1

2019

Legalizing Intelligence Sharing: A Consensus Approach

Brian Mund
Yale Law School

LEGALIZING INTELLIGENCE SHARING: A CONSENSUS APPROACH

Brian Mund*

ABSTRACT

Governments face a decision between balancing collective national security interests with individual privacy rights and strike that balance to different degrees. Only recently has public attention turned to the lack of transparency surrounding cross-border international intelligence sharing agreements. Foreign intelligence cooperation is necessary for effective security, but differing intelligence governance standards create tension between clashing privacy regimes. This Article proposes a pragmatic pathway forward in the form of a palatable intelligence-sharing framework that respects state sovereignty and security needs, while simultaneously establishing revolutionary privacy protections. This first-of-its-kind framework identifies and builds upon principles of international law to construct this practical framework. These principles are: 1) principle of legality; 2) principle of safeguarding against abuse; 3) principle of proportionality; 4) principle of transparency and oversight; 5) principle of notification and remedies; 6) principle of complementarity; 7) principle of good faith; and 8) an exigency exception.

* **Brian Mund** is a 2018 graduate of Yale Law School, where he received his Juris Doctor, and a 2013 graduate of the University of Pennsylvania, from which he received a Bachelor of Arts degree. He is grateful to Professor Michael Reisman and Asaf Lubin as well as the 2018 Salzburg Cutler Global Seminar participants for their feedback on previous drafts of this Article. All errors are the author's alone.

TABLE OF CONTENTS

INTRODUCTION

> *Suppose that Jane Doe shows up at our border with a valid visa, but after that visa was issued . . . her home country learns that she is associated with a terrorist organization but doesn't tell us.*[1]

On April 25, 2018, United States Solicitor General, Noel Francisco, defended President Donald Trump's third travel ban—which targets nationals from Iran, Libya, Yemen, Somalia, North Korea, and Venezuela—before the Supreme Court on the basis of inadequate information sharing.[2] Setting aside the merits of this particular order, the case shines a light onto the commonplace reality of cross-border information sharing. This snippet above reflects the larger reality that in today's world, cross-border information sharing plays a vital role in ensuring national security for many states. In other words, governments keep their nations safe through exchanges of intelligence data.[3]

---

[1] Transcript of Oral Argument at 8, Trump v. Hawaii, 138 S. Ct. 2392 (2018) (No. 17–965).

[2] Adam Liptak, *Supreme Court Allows Trump Travel Ban To Take Effect*, N.Y. TIMES (Dec. 4, 2017), https://www.nytimes.com/2017/12/04/us/politics/trump-travel-ban-supreme-court.html. Chad has since been removed from the list countries. *See also Trump* 138 S. Ct. at 2405 (2018) ("Invoking his authority under 8 U. S. C. §§1182(f) and 1185(a), the President determined that certain entry restrictions were necessary to "prevent the entry of those foreign nationals about whom the United States Government lacks sufficient information").

[3] What is data? Merriam-Webster provides the comprehensive definition that data is "information in digital form that can be transmitted or processed." While data is a plural noun, this Article follows the popular singular constructive use. *See Data*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/data (last visited Mar. 8, 2019). Privacy interests arise in data that contains personally identifiable information (PII), defined as "[a]ny representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." *See, e.g., Guidance on the Protection of Personal Identifiable Information*, U.S. DEP'T LABOR, https://www.dol.gov/general/ppii (last visited Mar. 7, 2019). While this definition of PII is fairly inclusive, Paul Schwartz and Daniel Solove identify that "[a]t the same time, there is no uniform definition of PII in information privacy law." Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy And A New Concept Of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1814 (2011).

Currently, countries share intelligence information through bilateral agreements.[4] Many of these agreements are secret and do not purport to be binding under international law.[5] In recent years, multinational intelligence exchange has continued to grow.[6] However, the public has only limited information regarding the extent and details of cooperative intelligence-sharing operations other than the fact that such cooperation exists.[7] For example, the Five Eyes Signal Intelligence Alliance, made up of the United States, the United Kingdom, Australia, Canada, and New Zealand operates according to the United Kingdom-United States Communication Intelligence (UKUSA) Agreement, but the last publically available version is from 1955.[8] Taken together, these signs indicate that improvements in international intelligence exchange since 9/11 have wrought "a qualitative change" in the nature of intelligence cooperation.[9]

---

[4] HANS BORN ET AL., MAKING INTERNATIONAL INTELLIGENCE COOPERATION ACCOUNTABLE 62 (2015).

[5] *Id.*

[6] *Id.* at 64; *see also* Didier Bigo et al., *National Security and Secret Evidence in Legislation and Before the Courts: Exploring the Challenges*, *in* EUR. PARL.: C.L., JUSTICE & HOME AFF. 8 (2014) (describing "a growing transnational exchange of intelligence"); Szabó & Vissy v. Hungary, App. No. 37138/14, Eur. Ct. H.R., Judgment, ¶ 78 (2016), http://hudoc.echr.coe.int/eng?i=001-160020 (noting that governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance."); S.C. Res. 1373 (Sept. 28, 2001) (calling all United Nations member states to "[e]xchange information in accordance with international and domestic law and cooperate on administrative and judicial matters to prevent the commission of terrorist acts.")

[7] Craig Forcese, The Collateral Casualties of Collaboration: The Consequence for Civil and Human Rights of Transnational Intelligence Sharing 6–11 (Mar. 5, 2009) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1354022 (explaining the difficulty to piece together the full scope and extent of intelligence arrangements because these agreements are so closely guarded).

[8] *See* Scarlet Kim et al., *The "Backdoor Search Loophole" Isn't Our Only Problem: The Dangers of Global Information Sharing*, JUST SEC. (Nov. 28, 2017), https://www.justsecurity.org/47282/backdoor-search-loophole-isnt-problem-dangers-global-information-sharing/; *see also* U.K.-U.S. Communications Intelligence Agreement, U.S.-U.K., May 10, 1955, https://www.nsa.gov/news-features/declassified-documents/ukusa/assets/files/new_ukusa_agree_10may55.pdf.

[9] Richard J. Aldrich, *Global Intelligence Co-operation versus Accountability: New Facets to an Old Problem*, 24 INTELLIGENCE & NAT'L SEC. 26, 30, 54 (2009).

Intelligence sharing has also fallen under increased scrutiny by the privacy rights advocacy community. In September 2017, Privacy International spearheaded a campaign along with the Center for Democracy & Technology, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the Open Technology Institute to "seek increased transparency for intelligence sharing arrangements" from over forty governments.[10] Specifically, the Privacy International coalition has pressed for transparency on intelligence sharing, and has also identified intelligence cooperation among "the Nine-Eyes (the Five Eyes plus Denmark, France, the Netherlands and Norway), the 14-Eyes (the Nine-Eyes plus Belgium, Germany, Italy, Spain and Sweden), and the 43-Eyes (the 14-Eyes plus the 2010 members of the International Security Assistance Forces to Afghanistan)."[11] Other identified multilateral intelligence sharing arrangements include EUROPOL between the EU member states, the Africa-Frontex Intelligence Community between European and African states, intelligence cooperation between eleven countries in the Great Lakes Region, the Shanghai Cooperation Organization between China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan,

---

[10] Letter from Gus Hosein et al., Exec. Director, Privacy Int'l, to Elizabeth B. Collins, Board Member, Privacy & Civ. Liberties Board, Re: Oversight of intelligence sharing between your government and foreign governments (Sep. 13, 2017), https://www.documentcloud.org/documents/4000688-US-Open-Letter-on-Intelligence-Sharing-and.html; *see also* PRIVACY INT'L, EVIDENCE ON THE DATA PROTECTION BILL AND PROPOSED AMENDMENTS FOR THE HOUSE OF COMMONS PUBLIC BILL COMMITTEE 6 (2018) (explaining that "[t]he Bill provides for almost unfettered powers for cross-border transfers of personal data by intelligence agencies without appropriate levels of protection.") https://publications.parliament.uk/pa/cm201719/cmpublic/dataprotection/memo/dpb07.pdf.

[11] *Privacy International Launches International Campaign For Greater Transparency Around Secretive Intelligence Sharing Activities Between Governments*, PRIVACY INT'L (Oct. 23, 2017), https://www.privacyinternational.org/press-release/51/privacy-international-launches-international-campaign-greater-transparency-around [hereinafter Privacy International]; *see also* Scarlet Kim et al., *Newly Disclosed Documents on the Five Eyes Alliance and What They Tell Us about Intelligence-Sharing Agreements*, LAWFARE (Apr. 23, 2018), https://www.lawfareblog.com/newly-disclosed-documents-five-eyes-alliance-and-what-they-tell-us-about-intelligence-sharing (describing pressure for US disclosure of secret intelligence agreements).

and an anti-Islamic State intelligence sharing coalition of Russia, Iraq, Iran, and Syria.[12]

This Article responds to the demand for greater intelligence sharing accountability by offering a detailed and thorough governmental intelligence cooperation framework. This type of pragmatic, compromising approach is sorely missing from a literature filled with idealistic yet wholly impractical measures. With intelligence sharing propelled under the public spotlight with renewed vigor in late 2017, the time is ripe for such an intervention. This Article offers a pragmatic pathway forward for governments and activists in the form of a palatable proposal that respects state sovereignty and security needs while simultaneously establishing revolutionary privacy protections.

The Article further emphasizes the distinct tension that arises from government intelligence sharing of personal information. This tension primarily arises when government intelligence agencies transfer information related to national security threats: specifically, cross-border intelligence transfers to combat serious crime and national security threats.[13] Government intelligence transfers occur most frequently among allied countries,[14] but as

---

[12] *See Human Rights Implications of Intelligence Sharing*, PRIVACY INT'L (Sept. 2017), https://www.privacyinternational.org/sites/default/files/2017-11/PI-Briefing-to-National-Intelligence-Oversight_0.pdf; Stephane Lefebvre, *The Difficulties and Dilemmas of International Intelligence* Cooperation, 16 INT'L J. INTELLIGENCE & COUNTERINTELLIGENCE 527, 529–534 (2003).

[13] Privacy-security tradeoff considerations are also engaged during inter-governmental law enforcement data sharing and involve information transfers to one another for the exchange of evidence and information in criminal and related matters. These transfers usually occur through the formalized process outlined within a Mutual Legal Assistance Treaty (MLAT). *See generally 2012 International Narcotics Control Strategy Report*, U.S. DEP'T OF STATE (Mar. 7, 2012) https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm (detailing United States' use of MLATs). A considerable literature has been emerging over the appropriate process for MLAT reform. *See infra* note 186. While MLAT reform poses an important step to strengthen the international data sharing regime, law enforcement sharing, and intelligence sharing are most appropriately addressed separately for reasons addressed *infra*, notes 211–286.

[14] *See, e.g.*, Data Protection Bill, 20 Mar. 2018, Parl Deb HL (2018) col. 161 (UK), https://hansard.parliament.uk/Commons/2018-03-20/debates/c72d5ec6-a472-4c53-be4c-8c80f291bd2f/DataProtectionBill(Lords)(FifthSitting) (quoting Victoria Atkins in saying that "[i]n the vast majority of cases, intelligence sharing takes place with

the *Trump v. Hawaii* oral argument transcript suggests, not exclusively.[15] These transfers directly engage profound questions with respect to the proper relationship between actions taken in the name of national security and ensuring appropriate privacy protections for the dissemination of private information. Intelligence sharing between foreign intelligence agencies provides tangible national security benefits. However, such benefits must be balanced against the costs to privacy and open expression.

The world of intelligence sharing is understandably opaque. Hans Born, Ian Leigh, and Aidan Wills provide a useful taxonomy for conceptualizing international intelligence cooperation, and this paper adopts their thoughtful framework.[16] Born *et al.* identifies five types of international intelligence cooperation: 1) information sharing, 2) covert operational cooperation, 3) hosting facilities and equipment, 4) training and capacity building, and 5) providing software and equipment.[17] This paper focuses on the first type: information sharing. Information sharing includes strategic information, operational information, and tactical information. Strategic information includes policy analyses related to foreign policy developments or larger security trends.[18] Operational information generally involves threat assessments of groups' or actors' current capabilities, and unlike policy-oriented strategic analyses, tends to be directed at security personnel. Finally, tactical information relates to the specifics relevant for current operations—the specific details necessary for answering the "who, what, where, when, and how."[19]

Shared intelligence information splits into two further subcategories: "raw intelligence" or an analyzed "end product."[20] Raw intelligence has not been altered from its initial collection form, whereas the "end product" has

---

countries with which the intelligence services have long-standing and well-established relationships.").

[15] *See generally* Transcript of Oral Argument, Trump v. Hawaii, 138 S. Ct. 2392 (2018) (No. 17–965).

[16] BORN ET AL., *supra* note 4.

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *Id.*

already received initial treatment by intelligence operatives. The sensitivity of the collection source will impact the likelihood of raw data sharing, as will the relationship between the two agencies. Lastly, the process of information sharing can manifest in two distinct forms. Most often, information sharing is "reactive," and results from *ad hoc* requests from a foreign partner for any information on a given subject.[21] However, close allies may also share information on an "automated basis."[22] These arrangements may rely on joint databases or other shared receptacles of gathered intelligence information.

I. EXISTENCE OF PRIVACY-SECURITY TRADEOFF

Throughout the world, people care deeply about their privacy. Common-law courts have long recognized the importance of privacy from governmental intrusion. This long-standing common law principle announces, "the house of every one is to him as his castle and fortress, as well for his defense against injury and violence as for his repose."[23] As expounded by American courts, the privacy right allows one "to retreat into his own home and there be free from unreasonable governmental intrusion."[24] For European countries, Article 8 of the European Convention on Human Rights grants "[e]veryone . . . the right to respect for his private and family life, his home and his correspondence."[25] Many other countries also protect the privacy of its citizens. For example, Articles 23–25 of the Russian Constitution grant

---

[21] *Id.*

[22] *Id.*

[23] Pavesich v. New England Life Ins. Co., 50 S.E. 68, 71 (1905).

[24] Kyllo v. United States, 533 U.S. 27, 31 (2001) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)

[25] *See* Convention for the Protection of Human Rights and Fundamental Freedoms, Art. 8, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter "European Convention on Human Rights"]. European Courts have also explicitly held that that private life "includes personal identity, such as a person's name, and that the protection of personal data is of fundamental importance to a person's enjoyment of his right to respect for private life." Case C-92/09, Volker und Markus Schecke GbR v. Land Hessen, 2010 E.C.R. I-11063, http://curia.europa.eu/juris/document/document.jsf?text=&docid=80291&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1680697.

substantial privacy rights, including the protection against "the collection, keeping, use and dissemination of information about the private life of a person."[26] Article 40 of the Constitution of the People's Republic of China notes that "freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law."[27] In August 2017, the Indian Supreme Court overturned its precedent and unanimously declared, "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution."[28] Notwithstanding this background of general respect for privacy rights, government security practices threaten to intrude upon citizens' rights.

However, the very purpose of privacy rights continues to be a source of debate among various countries. The debate over the contours and purpose of privacy rights does not map along a simple East-West or North-South divide; for example, scholars have recognized "two western cultures of privacy"[29] with fundamentally different approaches to privacy and surveillance.[30] Recent scholarship has also recognized that China's unique cultural and historical foundation of privacy have generated a wholly

---

[26] RUSSIAN CONST., art. 23–25, http://www.constitution.ru/en/10003000-03.htm.

[27] CHINESE CONST., March 14, 2004, art. 40, http://www.hkhrm.org.hk/english/law/const03.html.

[28] Justice K. S. Puttaswamy (Retd.) and Anr. v. Union Of India & Ors., (2017) Writ Petition (Civ.), No. 494 of 2012, http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

[29] *See generally* James Whitman, *The Two Western Culture of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151 (2004).

[30] *See* David Cole & Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy Across Borders*, 14 INT'L J. CONST. L. 220, 237 (2016). For an informative survey of 13 countries' surveillance and data privacy laws, *see generally* Peter Swire & DeBrae Kennedy-Mayo, *How Both The Eu And The U.S. Are "Stricter" Than Each Other For The Privacy Of Government Requests For Information*, 66 EMORY L. J. 617 (2017) http://law.emory.edu/elj/content/volume-66/issue-3/articles/both-eu-us-stricter-privacy-requests-information.html; Ira S. Rubinstein et al., *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 INT'L DATA PRIVACY L. 96 (2014), https://doi.org/10.1093/idpl/ipu004.

different conception of privacy.[31] These fundamentally different views of privacy have prevented the formation of any internationally accepted right to privacy or data protection.[32] Even among the subset of countries that recognize such rights, deep disagreement persists over the appropriate scope or content of those rights, and the appropriate role of courts in reviewing security practices.[33]

If the expansion of privacy rights were purely a positive-sum-game, then few would oppose the implementation of greater individual privacy protections. However, as alluded to above, privacy protections come at a cost to security interests, and vice versa.[34] Government security interests encourage information-gathering tactics that impose limitations on citizens' interests in their privacy and family life, as well as their "right to be let alone."[35] Furthermore, the fear of government surveillance may chill

---

[31] *See generally* Tiffany Li et al., *Saving Face: Unfolding the Screen of Chinese Privacy Law*, J. L. INFO. & SCI. (forthcoming), https://ssrn.com/abstract=2826087.

[32] *See, e.g.*, Bert-Jaap Koops & Morag Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law 1, 47 (Tilburg L. Sch., Research Paper No. 5/2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698263 (stating, in relevant part, that "there is no universally shared content for the right to privacy or data protection at the international level."); Data Protection Bill, 10 October 2017, Parl Deb HL (2017) col. 785 (UK), https://hansard.parliament.uk/Lords/2017-10-10/debates/A0271CAB-90BC-49BD-B284-664918EE70CA/DataProtectionBill(HL) (quoting the Earl of Lytton in saying, "[a]s regards international cross-jurisdictional data— I am thinking of beyond the EU—I wonder how successfully the proposed arrangements will carry forward in the longer term, bearing in mind that the world market contains numerous players who for their own purposes and advantage might not be that keen to match the standards we claim to set for ourselves.").

[33] *Id.*

[34] As former President Barack Obama put it, "You can't have 100% security and also then have 100% privacy and zero inconvenience, . . . we're going to have to make some choices as a society." Peter Nicholas & Siobhan Gorman, *Obama Defends Surveillance*, WALL ST. J. (June 8, 2013), https://www.wsj.com/articles/SB10001424127887324299104578531742264893564.

[35] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. R. 193, 193 (1890). *See also* Charter of Fundamental Rights of the European Union, art. 8, Oct. 10, 2012 O.J. (C 326) 02, http://fra.europa.eu/en/charterpedia/article/8-protection-personal-data (stating, in relevant part, that "[e]veryone has the right to the protection of personal data concerning him or her."). Such an approach views one's personal

individual freedoms of speech, assembly, and association.[36] On the other hand, privacy protective measures that reduce government access to information-gathering methods could hamstring efforts to identify and thwart dangerous threats to the societies' collective security interests.[37] Accordingly, the government mandate to ensure the safety of its citizenry requires the government to undertake some behaviors that intrude into the sphere of personal privacy.[38]

---

information as commensurate with ownership over one's identity and sense of self. Allowing governments to share that information can be deeply injurious to one's sense of identity. *See, e.g.*, Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1911 (2013), https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf (stating, in relevant part, that "[s]ubjectivity is a function of the interplay between emergent selfhood and social shaping; privacy, which inheres in the interstices of social shaping, is what permits that interplay to occur.").

[36] There are several famous examples from United States' jurisprudence. *See, e.g.*, United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 314 (1972) ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."); *see also* United States v. Jones, 565 U.S. 400, 416, 132 S. Ct. 945, 956, 181 L. Ed. 2d 911 (2012) (Sotomayor, J., concurring) ("[a]wareness that the Government may be watching chills associational and expressive freedoms."). Researchers have sought to show that the fear of government surveillance does in fact change citizen behavior. *See* Brynne O'Neal, *What Americans Actually Do When the Government Is Watching*, HUFFINGTON POST (Jul. 20, 2015), https://www.huffingtonpost.com/brynne-oneal/what-americans-actually-do-when-the-government-is-watching_b_7833408.html; *see also* BORN ET AL., *supra* note 4, at 45.

[37] [Irish] Data Prot. Comm'r, v. Facebook Ireland Ltd. & Maximillian Schrems [2016 No. 4809 P.], 40 (H. Ct.) (Ir.), http://www.europe-v-facebook.org/sh2/HCJ.pdf ("A degree of surveillance for the purposes of national security, counterterrorism and combating serious crime is vital for the safeguarding of the freedoms of all citizens of the union. This necessarily involves interference with the right to privacy, including data privacy.").

[38] As former FBI Agent Asha Rangappa explains, "[a]s any law enforcement official will tell you, criminals and spies don't show up on the doorstep of law enforcement with all of their evidence and motives neatly tied up in a bow. Cases begin with leads, tips, or new information obtained in the course of other cases. . . . However, anytime the FBI receives a credible piece of information that could indicate a potential violation of the law or a threat to national security, it has a legal duty determine whether a basis for further investigation exists." Asha Rangappa, *Don't Fall for the Hype: How the FBI's*

The privacy-security tradeoff is not a new phenomenon. In the prelude to the American independence, colonial Americans well understood the "difficult tradeoff between safety and freedom."[39] As Alexander Hamilton argued:

> The violent destruction of life and property incident to war; the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty, to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they, at length, become willing to run the risk of being less free.[40]

The challenge that Hamilton faced was the same difficulty that government decision makers continue to struggle with today: where to strike the appropriate tradeoffs between privacy and security.[41] As the British government recently declared, "There are circumstances where the processing of data is vital for our economy, our democracy and to protect us against illegality."[42] Today, the question facing states involves grappling with:

> how [do] we get the balance right between protecting the freedoms and civil liberties that underpin our functioning liberal democracy

---

Use of Section 702 Surveillance Data Really Works, JUST SEC. (Nov 29, 2017), https://www.justsecurity.org/47428/dont-fall-hype-702-fbi-works. Inevitably, some of these suspicions will not translate into actual threats to national security or even legal infractions. This necessary reality of overreach means that bulk data searches must be "adequately authorised and limited by domestic law." BORN ET AL., *supra* note 4, at 70. Presently, such protection "seems to be the exception rather than the norm". *Id.*

[39] Hamdi v. Rumsfeld, 542 U.S. 507, (2004) (Scalia, J., dissenting); see also Medina v. California, 505 U.S. 437, 443 (1992) (providing, in relevant part, that "[t]he Bill of Rights speaks in explicit terms to many aspects of criminal procedure, and the expansion of those constitutional guarantees under the open-ended rubric of the Due Process Clause invites undue interference with both considered legislative judgments and the careful balance that the Constitution strikes between liberty and order.").

[40] *Id.* (citing THE FEDERALIST No. 8, p. 33).

[41] *See* Eugene Volokh, *Liberty, Safety, and Benjamin Franklin*, WASH. POST (Nov. 11, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin (emphasizing that the "real challenge is in deciding which tradeoffs are wise and which are foolish.").

[42] Dep't Digital, Culture, Media & Sport, *Data Laws To Be Made Fit For Digital Age*, UK GOV. (Sep. 14, 2017), https://www.gov.uk/government/news/data-laws-to-be-made-fit-for-digital-age.

> while protecting that democracy from the various threats to our safety and well-being. The sophisticated use of new technologies by terrorist groups and organised crime means that we have to make a sober assessment of exactly what powers our police and security services need to combat the terrorist attack and disrupt the drug or people trafficker or the money launderer. The fact that those threats are often overlapping and interconnected makes granting powers and achieving appropriate checks and balances ever more difficult.[43]

When Hamilton considered this question, the debate concerned a wholly domestic issue. The Continental Congress had to engage in introspection and begin carving a tradeoff consonant with American values. The national nature of this decision meant that different sovereign countries could strike different tradeoffs without friction. However, the privacy-security tradeoff for modern, international intelligence sharing changes that paradigm.

States' national privacy-security balance generates difficult decisions when considering information-sharing arrangements with other governments. While the privacy concerns are considerable, state security interests mandate cooperative data sharing as a crucial component of state practice. Before exploring solutions to conflicting surveillance regimes, the sections below expand upon the privacy-security tension in cross-border intelligence sharing.

II. PRIVACY-SECURITY TRADEOFF FOR INTELLIGENCE SHARING

A. *Intelligence Sharing Raises Privacy Concerns*

As outlined above, domestic privacy protections play an important role in limiting government intrusion into the private lives of its citizens.[44]

---

[43] Data Protection Bill, 10 October 2017, Parl Deb HL (2017) col. 785 (UK), https://hansard.parliament.uk/lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL).

[44] *See, e.g.*, Myres S. McDougal et al., *The Intelligence Function and World Public Order*, 46 TEMP. L.Q. 365, 397 (1973) ("Much intelligence inevitably touches upon the private lives and pursuits of individuals and its dissemination is bound to have at least some adverse effects.").

Unchecked intrusion threatens to chill the important freedoms of speech, assembly, and association.[45] If these fears arise from one's own government surveillance, *a fortiori*, they are exponentially amplified by data sharing with foreign governments.[46] Every citizen enjoys national citizenship[47] and retains the peace of mind that their national government owes some obligations and fealty to protect the interests of their own nationals.[48] No such commitment exists for foreign government actors, and citizens have no reason to expect foreign governments to consider foreign citizens' interests when accessing personal data.[49] To the contrary, if a government receives private information that allows it to further its own national interests at the foreign citizen's expense, that government would assuredly do so. Thus, the government's data sharing practices with foreign governments jeopardize its citizens' private sense of security, a feeling further enhanced by foreign governments' freedom to further circulate the private information.[50]

Of course, one should not discount the possibility that not only will *fear* create chilling effects but that the private information might actually be used to stifle the above-mentioned rights. Regimes may utilize shared information

---

[45] *See supra* notes 23–36.

[46] *See, e.g.*, Privacy Int'l, *supra* note 11 ("States may share intelligence with States known for violating international law, ... Such sharing can place individuals in those States at particular risk.").

[47] *See, e.g.*, United Nations Convention on the Reduction of Statelessness art. 1, Aug. 30, 1961, 989 U.N.T.S. 175.

[48] *See, e.g.*, Myres S. McDougal et al., *Nationality and Human Rights*, 83 YALE L. J. 900, 960 (1974) (stating that "on the transnational level[,] nationality is the right to have protection in rights").

[49] *See, e.g.*, Robin Simcox, *Europe, Stop Trying to Make 'Intelligence Sharing' Happen*, FOREIGN POL'Y (Apr. 14, 2016), http://foreignpolicy.com/2016/04/14/europe-stop-trying-to-mak-brussels-paris-bombings ("Brits may have become used to the CCTV cameras and Automatic Number Plate Recognition technology that allows their own government to monitor their travel—but they would be considerably more dubious about letting the Germans and the French do the same.").

[50] *See generally* Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473 (2016), http://jnslp.com/wp-content/uploads/2016/11/Law_Enforcement_Access_to_Data_Across_Borders_2.pdf (detailing ways through which collection of private information can stifle rights and freedoms).

to monitor political dissidents or regime opponents living as part of a foreign diaspora community.[51] Such privacy and even safety concerns may pose a barrier to data sharing agreements with countries bearing shaky human rights records.[52] Even when shared information would not lead to concrete harm, countries may also hesitate to share information to partners with poor privacy safeguards due to the belief that the mere access to the private information constitutes severe dignitary harm.

Similar considerations also weigh in favor of caution before utilizing shared data received from an intelligence partner. If the intelligence partner does not honor the same degree of privacy as the home state, the home state may fear complicity in privacy or human rights violations.[53] The "Originator Rule" allows the original collector of information to govern the subsequent downstream flow of the information.[54] If an intelligence agency receives information from a foreign counterpart, the information originator may choose to not include the sources or procedures by which the agency acquired this information. As such, the recipient agency may unknowingly utilize private information that was unlawfully gathered under foreign laws.

Agencies can also take advantage of disparate protective regimes through the deliberate use of a "revolving door" tactic. The "revolving door" describes a mechanism through which government intelligence agencies rely on foreign

---

[51] BORN ET AL., *supra* note 4, at 45. By the same token, however, sharing information about domestic dissidents might have a significantly *smaller* chilling effect. American political dissidents might fear retaliatory action by the United States yet would probably be far less concerned about repercussions from a removed country like China. *See* Stephen J. Schulhofer, *An International Right to Privacy? Be Careful What You Wish For*, 14 INT'L J. CONST. L. 238 (2016), https://doi.org/10.1093/icon/mow013; Ashley Deeks, *An International Legal Framework for Surveillance*, VA. J. INT'L L. 291, 346 (2015) https://ssrn.com/abstract=2490700; Asaf Lubin, *'We Only Spy on Foreigners': The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance*, 18 CHI. J. INT'L L. 502, 534 (2018) https://ssrn.com/abstract=3008428 ("Chinese, French, and Russian intelligence agents do not have the time or inclination to harass random Americans, nor the capability as long as Americans remain in the United States.").

[52] Lefebvre, *supra* note 12, at 535.

[53] AIDAN WILLS, UNDERSTANDING INTELLIGENCE OVERSIGHT 25 (2010), http://www.dcaf.ch/sites/default/files/publications/documents/IntelligenceOversight_en.pdf.

[54] Lubin, *supra* note 51.

collection to collect information that they could not have legally collected under their domestic legal frameworks.[55] This is not merely an abstract concern. Part 0 describes the United States' lack of privacy protection for non-U.S. citizens located abroad. Insofar as foreign intelligence partners such as the Five Eyes coalition have access to United States intelligence databases, U.S. overseas collection practices may directly facilitate a legal quagmire for those foreign agencies.[56] While the bulk collection may have been legal under United States law, these partners might not have legal authorization to collect such information. The revolving door is not a one-way street: the Wall Street Journal has also reported that Europeans have also collected intelligence information for American intelligence agencies.[57] As David Cole and Federico Fabrinni note, "Reports of cooperation and mass intelligence sharing between the NSA and the General Communication Headquarters (GCHQ), the United Kingdom's surveillance agency, make these concerns even more immediate."[58] Thus, intelligence sharing agreements should account for the legitimate privacy interests implicated in inter-governmental data transfers.

B. Effective Security Requires Intelligence Sharing

Policing and counterterrorism efforts necessarily depend on cross-border data sharing.[59] The modern era has ushered in an age of advanced communications technologies and increasingly sophisticated threats that do not confine themselves to national borders. In the globalized 21st century, effective national security practices require not only data access among national law

---

[55] *Id.*

[56] *See* Kim et al., *supra* note 8.

[57] Adam Entous & Siobhan Gorman, *Europeans Shared Spy Data With U.S.*, WALL ST. J. (Oct. 29, 2013), https://www.wsj.com/articles/us-says-france-spain-aided-nsa-spying-1383065709.

[58] Cole & Fabbrini, *supra* note 30, at 222.

[59] Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 742 (2016) (stating, in relevant part, that "Governments seek lawful access to Internet data for a host of reasons, including counterterrorism operations, immigration control, and many other administrative matters.").

enforcement and intelligence agencies but also cooperative data sharing with international intelligence partners.[60]

In today's global economy, the idea of data fails to comport with traditional borders, and security threats have adopted a transnational nature.[61] As Professor Jennifer Daskal points out, "The ease and speed with which data travels across borders, the seemingly arbitrary paths it takes, and the physical disconnect between where data is stored and where it is accessed critically test these foundational premises [of territoriality]."[62] In a world of non-territorial data, blocking foreign security data streams can have significantly adverse consequences. As President Obama observed, "[E]merging threats from terrorist groups and the proliferation of weapons of mass destruction place new and in some ways more complicated demands on our intelligence agencies. Globalization and the Internet made these threats more acute, as technology erased borders and empowered individuals to project great violence . . .."[63] One Irish Court recently recognized that limitations on legal

---

[60] *Id.* at 745 ("This is striking: a police officer now must cross an international border in order to do her job, whereas twenty or even ten years ago, the same officer might have been able to investigate a routine crime like kidnapping without leaving her country. Just as crime has become increasingly global, evidence gathering has followed suit."). This trend has long been in the works. *See* McDougal et al., *supra* note 44, at 424 (noting that increasing global interrelation has "rendered intelligence gathering a global operation requiring more institutional and ad hoc cooperation across political boundaries.").

[61] *But see* Woods, *supra* note 59, at 763 ("At a deep conceptual level, data is not as novel as the data exceptionalists suggest. None of the features that are thought to make data novel are in fact novel-whether the features are considered individually or as a whole-and in fact, data is an easier case than some other assets because data has a physical location wherever it is stored").

[62] Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015).

[63] Ashley Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 622 (2016) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2768339 (citing *Remarks by the President on Review of Signals Intelligence*, WHITE HOUSE OFFICE PRESS SEC'Y (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence).

security sharing "has potentially extremely significant implications for the safety and security of residents within the European Union."[64]

This reflects a larger truth that as transnational integration has developed, so too has state susceptibility to intervention or interruption by individuals located around the world. As criminal activity takes an increasingly international flavor,[65] domestic information alone proves insufficient to provide safety in the twenty-first century. This position does not merely reflect theoretical rhetoric arising from the desire to shape the modern global citizen. Rather, this position has been cemented by empirical experience: it is widely accepted among the global intelligence community that international data sharing incidents have contributed to saving many lives.[66] To highlight one well-cited example, Canada's refusal to accept Indian intelligence information regarding a threat of homegrown Canadian Sikh extremist nationalists resulted in the destruction of Air India Flight 182 and cost 329 lives.[67]

In addition to preventing the loss of life, intelligence-sharing agreements provide a number of important benefits. Intelligence sharing with foreign governments helps provide a more complete picture of often-cryptic circumstances that allow "military commanders, law enforcement officials,

---

[64] [Irish] Data Prot. Comm'r, v. Facebook Ireland Ltd. & Maximillian Schrems [2016 No. 4809 P.J, 3 (H. Ct.) (Ir.), http://www.europe-v-facebook.org/sh2/HCJ.pdf.

[65] For example, "between October 2014 and September 2015, the UK Financial Intelligence Unit (UKFIU) received 1,566 requests from international partners for financial intelligence. Of these, at least 800 came from EU Member States. In the same period, the UKFIU proactively disseminated 571 pieces of financial intelligence to international financial intelligence units, 200 of which went to Europol." *The Exchange and Protection of Personal Data: A Future Partnership Paper*, HM GOV'T (2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf; *see also* Woods, *supra* note 59, at 744–745 (2016) (presenting U.K. Government Requests for Internet Data from Major U.S. Service Providers in 2014).

[66] *See, e.g.*, BORN ET AL., *supra* note 4, at 33 ("[I]nternational intelligence cooperation can help to safeguard the right to life, and it can prevent serious threats to public safety. It is widely accepted that information sharing has contributed to the prevention of numerous terrorist attacks over the past decade, saving many lives.")

[67] *See id.* at 41 (citing COMMISSION OF INQUIRY INTO THE INVESTIGATION OF THE BOMBING OF AIR INDIA FLIGHT 182, 422–31 (2010)).

and policymakers to improve the quality of their decision making."[68] Additionally, data sharing provides for significant cost-savings and enables operational efficiencies. Data sharing delivers benefits in the division of labor, reducing the burden of duplicative investigative efforts, and leveraging specialized areas of expertise.[69] Take the example of human intelligence.[70] As the self-proclaimed Islamic State loses the last of its territory and resources, many fear that it will increasingly turn its focus to conducting international terrorism.[71] As such, governments who fear that they are potential targets will seek to place clandestine operatives within the organization or recruit informants. Such measures are extremely costly, and the duplication of effort may itself compromise the efficacy of individual missions. Moreover, certain governments will have comparative advantages—in this scenario, Middle Eastern governments will likely have more native language speakers and citizens with plausible ties to the region or conflict. At first glance, the ISIS case might seem distinguishable from the privacy concerns explored in this Article. However, even in this extreme scenario of the Islamic State, the Islamic State's international ambitions involve cross-border communications and association with and surveillance of individuals located around the world. When intelligence agencies can engage in information sharing, they benefit from the collective efficiencies.

---

[68] *Id.* at 34.

[69] *Id.* at 36 ("Close allies can work to avoid duplication of information collection efforts . . .. It may be easier for a service to work with a foreign partner whose intelligence officials and/or agents share these [specialized] characteristics"); Janine McGruddy, *Multilateral Intelligence Collaboration and International Oversight*, 6 J. STRATEGIC SEC. 214, 215 (2013) http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1317&context=jss ("No one country can effectively cover all the areas of interest that their intelligence collection requirements demand.")

[70] Human Intelligence (HUMINT) is defined by the Central Intelligence Agency as "any information that can be gathered from human sources." *INTelligence: Human Intelligence*, CENT. INTELLIGENCE AGENCY (last updated Apr. 30, 2013), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html.

[71] *See, e.g.*, Daniel Byman, *Beyond Iraq and Syria: ISIS' Ability to Conduct Attacks Abroad*, LAWFARE (Jun. 15, 2017, 11:14 AM), https://www.lawfareblog.com/beyond-iraq-and-syria-isis-ability-conduct-attacks-abroad ("This loss of territory and resources, however, increases the Islamic State's desire to conduct international terrorism.").

Intelligence sharing practices also lead to security improvements by effectuating peer review.[72] The nature of intelligence-sharing work can often insulate such practices from substantive agency review by other areas of the government. Through coordination with foreign government agencies, intelligence sharing establishes an avenue for an outside party to provide the intelligence agency with professional feedback. In doing so, intelligence-sharing agreements play an invaluable role in providing an objective and critical review of practices that lay "largely shielded" from external review.[73] While peer review provides a helpful informal model for intelligence feedback, it should not serve as the only source of oversight—an issue that receives extensive attention *infra*.

Finally, intelligence-sharing agreements permit governments to control the external information flow to other governments. Through such arrangements, governments can tailor the amount of information that they share with partners and can withhold sensitive material or titrate the circumstances in which they distribute such information. Cooperation can limit the degree to which foreign governments expend the resources to surveil non-citizens, thereby decreasing the risk of incidental foreign espionage threatening national security. These positive externalities of lessened foreign government espionage have encouraged even privacy advocates to push for data sharing regimes motivated by the belief that agreements will bolster citizens' protections against foreign government surveillance.[74]

---

[72] *See* Deeks *supra* note 63, at 640.

[73] BORN ET AL., *supra* note 4, at 36 ("Exchanging information and intelligence analyses with foreign partners can provide services with alternative perspectives on key issues and help them to challenge their own assumptions . . . the professional criticism that foreign partners can provide may be invaluable. Accordingly, services with close relationships will sometimes solicit comments on their strategic analyses.")

[74] *See* Cole & Fabbrini, *supra* note 30, at 236–37.

III. COUNTRIES STRIKE DIFFERENT PRIVACY-SECURITY BALANCES FOR NATIONAL INTELLIGENCE REGIMES

While popular imagery may paint a privacy-loving Europe and a security-obsessed United States, the reality is that when it comes to government surveillance, experts have recognized that "[s]afeguards under American law, for all their shortcomings, are far more robust than those now found or likely to emerge elsewhere," including in Europe.[75] European Union member states themselves hold widely varying views on the appropriate tradeoff balance on "such fundamental issues as the required level of suspicion, the role of suspect-specific judicial approval ex-ante, and the degree to which transparency and oversight."[76]

Taken holistically, EU law provides substantially more protection against government surveillance in three ways. First, it does not accept the third-party doctrine found in American jurisprudence, which robs individuals of a reasonable expectation of privacy—in other words, a privacy interest—in information that has been revealed to a third party.[77] The third-party doctrine has led American courts to reject a privacy interest in information given to a third party "even if the information is revealed on the assumption that it will be used only for a limited purpose."[78] The EU also imposes greater privacy

---

[75] Schulhofer, *supra* note 51, at 245. *See, e.g.*, Entous & Gorman, *supra* note 57, (statement of Rep. Mike Rogers) ("[The U.S. is] the only intelligence service in the world that is forced to go to a court before they even collect on foreign intelligence operations, which is shocking to me.").

[76] Schulhofer, *supra* note 51, at 245 ("There is wide variation, even among Western democracies, on such fundamental issues as the required level of suspicion, the role of suspect-specific judicial approval *ex ante*, and the degree to which transparency and oversight are relaxed in the national security context.").

[77] *Id.*

[78] United States v. Miller, 425 U.S. 435, 443 (1976). However, the United States jurisprudence on the third-party doctrine may be shifting for online information. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018) (limiting the scope of third-party doctrine by requiring a warrant for cell phone geo-location data lasting longer than a week); *see also* Brian Mund, *Social Media Searches and the Reasonable Expectation of Privacy*,

restrictions on the private sector, including limitations on the retention and use of data and has recognized a right to be forgotten.[79] The EU is also subject to the European Court of Human Rights (ECtHR), where the Court has built a considerable foundation for privacy protection, including a right against secret monitoring of postal and telephonic communications,[80] real-time communications interceptions,[81] and bulk data collection.[82] However, the ECtHR maintained wide discretion to state actors by granting a "margin of appreciation" in the national security and surveillance context.[83]

That is not to say that the United States is insensitive to privacy concerns; the central understanding of American privacy arises from the notion of freedom from state surveillance.[84] In three other ways, American law provides more privacy protections than the EU for government intelligence. First, while American law requires FISA authorization, EU law does not require judicial oversight.[85] Second, EU law does not require individualized suspicion for intelligence searches, which allows for greater bulk collection flexibility than is allowed in the U.S.[86] Third, EU law lacks "the detailed specificity of the US

---

19 YALE J. L. & TECH. 238, 256-57 (2017) http://yjolt.org/sites/default/files/mund19yjolt238_0.pdf (arguing that the U.S. Supreme Court has indicated a willingness to reconsider the third party doctrine for digital information).

[79] Schulhofer *supra* note 51, at 249.

[80] Klass v. Germany, App. No. 5029/71, Eur. Ct. H.R. (ser. A), Judgment (1978), http://hudoc.echr.coe.int/eng?i=001-57510.

[81] Malone v. United Kingdom, App. No. 8691/79, (1984) Eur. H.R. Rep. 14 (telephone interception); Copland v. United Kingdom, App. No. 62617/00, Eur. Ct. H.R., Judgment (2007), http://hudoc.echr.coe.int/eng?i=001-79996 (email interception).

[82] Rotaru v. Romania, App. No. 28341/95, Eur. Ct. H.R., Judgment (2000), http://hudoc.echr.coe.int/eng?i=001-58586; Marper v. United Kingdom, Apps. No. 30562/04 & 30566/04, Eur. Ct. H.R., Judgment (2008), http://hudoc.echr.coe.int/eng?i=001-90051.

[83] Cole & Fabbrini, *supra* note 30, at 227.

[84] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L. J. 1151, 1211–13 (2004), https://www.yalelawjournal.org/pdf/246_ftn7jo8w.pdf ("Suspicion of the state has always stood at the foundation of American privacy thinking.").

[85] Schulhofer, *supra* note 51, at 249.

[86] *Id* at 249–50.

Foreign Intelligence Surveillance Act (FISA)," which has left national security practices largely unregulated.[87]

However, the U.S. Fourth Amendment's protection against "unreasonable searches and seizures"[88] is not absolute, and the United States has shifted towards a greater security emphasis in the aftermath of the September 11 attacks. Most notably, the USA PATRIOT Act[89] has realigned the balance between the government and American citizens over the scope of reasonable privacy intrusions for national security purposes.[90] The PATRIOT Act included provisions that added a broad new definition of domestic terrorism under 18 U.S.C. § 2331[91] and allowed for delayed notice for certain searches and interceptions,[92] thereby facilitating extended covert operations.[93] Furthermore, the United States has extended Fourth Amendment procedural protections for domestic national security gathering[94] and has prevented the bulk data collection of all American telephone metadata records.[95] The United States offers much less protection to non-U.S. persons located abroad and has

---

[87] *Id.* at 250.

[88] U.S. CONST. Amend. IV.

[89] Pub. L. No. 107-56, § 1, 115 Stat. 272, 272–75.

[90] Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy under the USA Patriot Act*, 80 DENV. U. L. REV. 375, 379 (2002) ("The PATRIOT Act attacks the balance between the government and the individual by a systematic circumvention of established doctrine and procedures guarding against unreasonable governmental intrusion").

[91] *See* 18 U.S.C. § 2331; Patriot Act, H.R. 3162, 107th Cong. § 802 (2001).

[92] 18 U.S.C. § 3103(a).

[93] *USA Freedom Act: What's In, What's Out*, WASH. POST (Jun. 2, 2015), https://www.washingtonpost.com/graphics/politics/usa-freedom-act (stating that the USA Freedom Act reauthorized the PATRIOT Act while modifying some of the government's bulk data collection powers). *See generally* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 267 (2015), https://www.congress.gov/bill/114th-congress/house-bill/2048?q={%22search%22%3A[%22\%22hr2048\%22%22]}.

[94] United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 321 (1972) (holding government's national security concerns "do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance.").

[95] *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 796 (2d Cir. 2015) (interpreting §215 of the PATRIOT Act, 50 U.S.C. § 1861, to not authorize bulk data collection of American telephone records).

authorized extensive foreign collection data collection, even if the data also captures communications concerning persons located within the United States.[96]

The United States and Europe also differ in their approach to judicial review.[97] The European Union tilts heavily towards judicial engagement to protect individual privacy rights.[98] The contrast between the United States and European Union approach on the scope of judicial reviewability shines through a conclusion by the United States Foreign Intelligence Surveillance Court of Review (FISCR). Rather than allow substantive privacy interests to narrow legitimate national security methods, the FISCR judges instead recognized that "where the government has instituted several layers of

---

[96] United States v. Mohamud, 2014 WL 2866749, at *15 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420, 440 (9th Cir. 2016) ("The § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's communications with the extraterritorial target would be lawful."). *See also* Redacted, 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011) (providing, in relevant part, that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."). President Obama's Presidential Policy Directive 28 added additional safeguards for non-U.S. citizens located abroad and required that "signals intelligence activities must take into account that all persons should be treated with dignity and respect[.]" *See also Presidential Policy Directive No. 28, Signals Intelligence Activities* § 1 (Jan. 17, 2014) [hereinafter PPD-28], https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[97] This difference has been characterized as a "ballot-box democracy" in the U.S. versus a "fundamental rights" model of judicial review in Europe. *See* Francesca Bignami & Giorgio Resta, *Human Rights Extraterritoriality: The Right to Privacy and National Security Surveillance* at 19, *in* EYAL BENVENISTI & GEORG NOLTE, THE RIGHT TO PRIVACY AND NATIONAL SECURITY SURVEILLANCE IN COMMUNITY INTERESTS ACROSS INTERNATIONAL LAW (forthcoming), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=2562&context=faculty_publications.

[98] *See, e.g.*, Joined Cases C-293/12 and C-594/12, Digital Rights Ireland & Others v Minister for Communications, Marine & Natural Resources and Others, E.C.J., Judgment (Grand Chamber Apr. 8, 2014), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN (holding that "EU legislature's discretion is reduced" because of the fundamental right to respect for private life, the government's stated legitimate interest in national security notwithstanding.).

serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its efforts to protect national security should not be frustrated by the courts."[99]

Neither the United States nor the European Union represents the full range in which states establish their privacy-security tradeoff. For example, Japan has traditionally sat at the extreme "privacy" end of the privacy-security spectrum.[100] The Japanese government's ability to engage in surveillance and interception practices has been highly curtailed, including for national security purposes.[101] Japan has a wiretap law, but "Japanese culture strongly opposes government interceptions, and the authority is rarely used."[102] Until June 2017, Japan did not have a statutory basis for authorizing communications interceptions for counter-terrorism purposes.[103] However, Japan's robust privacy anti-interception laws do not translate to a complete lack of authorization for counter-terror activity. In 2016, the Japanese Supreme Court granted $880,000 to Muslim plaintiffs for privacy violations related to a leak of police files that revealed blanket surveillance of religious Muslims in Japan.[104] Nevertheless, Japan's Supreme Court affirmed a lower

---

[99] *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

[100] *See* Rubinstein et al., *supra* note 30, at 104 ("At the opposite extreme, Japan and Brazil are notable for the severe limits they impose on interceptions undertaken for foreign intelligence security purposes.").

[101] *Id.*

[102] *Id.* at 109 ("Japanese society strongly disfavours the use of wiretaps and the number of communications intercepts is miniscule."). *See also* Toshimaru Ogura, *Toward Global Communication Rights: Movements Against Wiretapping and Monitoring in Japan*, TRANSNATIONAL INSTITUTE (2018), https://www.tni.org/en/archives/act/2691 (last visited Oct. 11, 2018).

[103] Andy Sharp, *Abe Passes Controversial Bill Boosting Japan Surveillance Powers*, BLOOMBERG (Jun. 14, 2017 10:06 PM), https://www.bloomberg.com/news/articles/2017-06-15/abe-passes-controversial-bill-boosting-japan-surveillance-powers; Rubinstein et al., *supra* note 30, at 109 ("Japanese law lacks any statutory basis for authorizing wiretaps for counter-terrorism purposes.").

[104] Ian Monroe, *Top Court Green-Lights Surveillance of Japan's Muslims*, AL JAZEERA (Jun. 29, 2016), http://www.aljazeera.com/news/2016/06/top-court-green-lights-surveillance-japan-muslims-160629040956466.html.

court ruling permitting intelligence profiling and surveillance as "necessary and inevitable" to guard against the threat of international terrorism.[105]

At the other end of the spectrum, China and India heavily subordinate privacy interests to possible security needs in a way that neither the United States, the European Union, nor Japan would find appropriate. Both China and India are distinguished by their "almost total" lack of privacy protection from government monitoring and oversight. In India, the Indian Intelligence Bureau (IB) faces little public accountability.[106] In fact, the IB, which has existed since 1887, might not even have any legislative basis in modern Indian law.[107] The Indian government has also bolstered its surveillance capabilities through establishing a Central Monitoring System that enables government interception of emails, chats, voice calls and text messages without the assistance of third party service providers.[108] In addition, the Indian government has over 1.18 billion citizens[109] in its Aadhaar identification system based on biometric and demographic information and has disabled encryption between telephones and network stations, which facilitates government interception of communications transmissions.[110] The

---

[105] *Id.*

[106] Pranesh Prakash, *How Surveillance Works in India*, N.Y. TIMES (Jul. 10 2013, 2:29 AM), https://india.blogs.nytimes.com/2013/07/10/how-surveillance-works-in-india (stating that "[n]o intelligence agency in India has been created under an act of Parliament with clearly established roles and limitations on powers, and hence there is no public accountability whatsoever.").

[107] *See Subramanium to Katju: The Dangerous Elevation of the IB Report*, FIRST POST (Jul. 24, 2014), http://www.firstpost.com/india/subramanium-to-katju-the-dangerous-elevation-of-the-ib-report-1631981.html (noting that the IB is "agency established under an administrative order without any constitutional or statutory identity"). *See also Explain Intelligence Bureau's Legality, HC Tells Centre*, TIMES INDIA (Mar. 26, 2012), https://timesofindia.indiatimes.com/india/Explain-Intelligence-Bureaus-legality-HC-tells-Centre/articleshow/12408605.cms.

[108] Rubinstein et al., *supra* note 30, at 98; Leo Mirani, *Think US snooping is bad? Try Italy, India or . . . Canada*, QUARTZ (Jun. 10, 2013), https://qz.com/92648/think-us-snooping-is-bad-try-italy-india-or-canada.

[109] Unique Identification Authority of India, *Welcome to AADHAAR Dashboard*, GOV'T INDIA, https://uidai.gov.in/aadhaar_dashboard (last visited Feb. 28, 2019).

[110] *See generally* Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its*

government has wide discretion in utilizing this information for national security and other "public interest" purposes.[111] While a 1996 Supreme Court decision recognized that wiretapping constitutes an invasion of privacy,[112] the Indian government retains relatively wide discretion in collecting and utilizing information for national security and other "public interest" purposes.[113] Finally, India's laws grant procedural review by a committee of the law enforcement official's colleagues but critics have questioned its procedural credibility.[114]

China grants broad security powers to its security forces. As China scholar James Fry notes, "there are only a few legal limitations on the authorities when it comes to Internet surveillance, with the vast majority of laws providing the authorities many express powers over content censorship."[115] The Chinese Ministry of Public Security has undertaken the ambitious "Police Cloud" project, which, similarly to the Indian Aadhaar, collects a vast amount of information tied to citizens' unique national identification number.[116] China has also installed over 20 million cameras in

---

Impact on National Security and Consumer Privacy, 28 HARV. J. L. & TECH. 1 (2014), https://ssrn.com/abstract=2437678.

[111] Rhyea Malik & Subhajit Basu, *India's Dodgy Mass Surveillance Project Should Concern Us All*, WIRED (Aug. 25, 2017), http://www.wired.co.uk/article/india-aadhaar-biometrics-privacy; Prashant Reddy, *Data Protection: Can India Overcome the Spy-Security State and Big Tech To Enact a Strong Law?*, SCROLL (Aug. 22, 2017), https://scroll.in/article/846946/data-protection-can-india-overcome-the-spy-security-state-and-big-tech-to-enact-a-strong-law. *See also Data Protection Laws of the World: India*, DLA PIPER (Jan. 24, 2017), https://www.dlapiperdataprotection.com/index.html?t=law&c=IN (stating that "[t]here is no specific legislation on privacy and data protection in India.").

[112] *See* Prakash, *supra* note 106; Bhairav Acharya, *Mastering the Art of Keeping Indians Under Surveillance*, WIRE (May 30, 2015), https://thewire.in/2756/mastering-the-art-of-keeping-indians-under-surveillance.

[113] *See supra* note 109.

[114] *See* Acharya, *supra* note 112.

[115] James D. Fry, *Privacy, Predictability And Internet Surveillance In The U.S. And China: Better The Devil You Know?*, 37 U. PA. J. INT'L L. 419, 478 (2016), http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1910&context=jil.

[116] *China: Police 'Big Data' Systems Violate Privacy, Target Dissent*, HUMAN RIGHTS WATCH (Nov. 19, 2017), https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent.

the past few years as means of more closely monitoring its population.[117] With its extensive infrastructure, China has also introduced real-time facial recognition tracking[118] as well as voice recognition forensics for unidentified targets in phone conversations.[119] Chinese policies have also generated less expectation of privacy among the Chinese public. In one recent study, only 50 percent of Chinese consumers acknowledged the need for caution in sharing personal information online, and reflected a "more cavalier approach" towards data privacy among Chinese citizens.[120] In contrast, the average acknowledgment of data privacy caution in ten other countries exceeded 75 percent.[121] The Washington Post reports that spying in China is so pervasive that government officials often spy upon one another—leading to a practice of hugging at the beginning of meetings in order to pat down their counterparts for hidden microphones.[122]

China's trajectory appears to continue empowering widespread national security surveillance activity. China's Anti-Terrorism Law (ATL) requires telecommunication and Internet providers within Chinese jurisdiction to

---

[117] Frank Langfitt, *In China, Beware: A Camera May Be Watching You*, NAT'L PUB. RADIO (Jan. 29, 2013), https://www.npr.org/2013/01/29/170469038/in-china-beware-a-camera-may-be-watching-you.

[118] Ms. Smith, *Skynet in China: Real-life 'Person of Interest' spying in real time*, CSO ONLINE (Sep. 28, 2017), https://www.csoonline.com/article/3228444/security/skynet-in-china-real-life-person-of-interest-spying-in-real-time.html.

[119] *See China: Voice Biometric Collection Threatens Privacy*, HUMAN RIGHTS WATCH (Oct. 22, 2017), https://www.hrw.org/news/2017/10/22/china-voice-biometric-collection-threatens-privacy.

[120] *See* George G. Chen & Tiffany G. Wong, *Waiting for China's Data Protection Law*, DIPLOMAT (Aug. 12, 2017), https://thediplomat.com/2017/08/waiting-for-chinas-data-protection-law. *See also* Peter Fuhrman, *Government Cyber-Surveillance is the Norm in China—And Its Popular*, WASH. POST (Jan. 29, 2016), https://www.washingtonpost.com/opinions/cyber-surveillance-is-a-way-of-life-in-china/2016/01/29/e4e856dc-c476-11e5-a4aa-f25866ba0dc6_story.html (stating that "none [of my Chinese friends] expressed the slightest quibble about their government knowing where they travel or when they receive international calls.").

[121] *See* Chen & Wong, *supra* note 120.

[122] Max Fisher, *Chinese Government Officials Are Constantly Wiretapping And Spying On One Another*, WASH. POST (Feb. 13, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/02/19/chinese-government-officials-are-constantly-wiretapping-and-spying-on-one-another.

grant data access and decryption support to government authorities under the ambit of national security.[123] Given the government's sweeping authority to take "all necessary" steps to guard China's sovereignty,[124] the ATL effectively grants access to any and all locally stored data that the Chinese government might want.[125] Finally, an updated Intelligence Law promotes a similar purpose, broadly allowing Chinese security officials to "make inquiries of any individuals as part of their intelligence-gathering, and to examine their reference materials and files [and] commandeer the communications equipment, transportation, buildings, and other facilities of individuals as well as organizations and government organs."[126]

In short, countries ranging from Japan, the European Union, the United States, India and China all display a wide array of preferences and values regarding their internal balance between privacy and national security interests. In the age of transnational data, these balances necessarily bleed

---

[123] Courtney M. Bowman et al., *A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization*, PROSKAUER (May 9, 2017), https://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization (stating that decryption assistance has not included a requirement to surrender decryption keys); Alyssa Abkowitz & Eva Dou, *Apple to Build China Data Center to Meet New Cybersecurity Law*, WALL ST. J. (Jul. 12, 2017), https://www.wsj.com/articles/apple-to-build-china-data-center-to-meet-new-cybersecurity-law-1499861507; Dante D'Orazio, *China Passes Controversial Anti-Terrorism Law To Access Encrypted User Accounts*, VERGE (Dec. 27, 2015), https://www.theverge.com/2015/12/27/10670346/china-passes-law-to-access-encrypted-communications (stating that "[t]he new law does not require that companies operating in China hand over encryption keys.").

[124] This *carte blanche* is conferred pursuant to China's National Security Law. *See* Bowman et al., supra note 123.

[125] *See* D'Orazio *supra* note 123 ("President Obama raised his concerns over draft regulations with China's President Xi Jinping, saying that the rules amounted to a dangerous backdoor to internet services.").

[126] Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (Jul. 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; *China Activists Fear Increased Surveillance With New Security Law*, REUTERS (May 25, 2017), https://www.reuters.com/article/us-china-security-int/china-activists-fear-increased-surveillance-with-new-security-law-idUSKBN18M09U.

beyond state borders and create difficult questions for intelligence sharing between various agencies. The next section explores some of the barriers to intelligence sharing that have arisen in the face of this tradeoff.

IV. BARRIERS TO CROSS-BORDER INTELLIGENCE REGIME

The privacy-security value disparity has led to pressure on intelligence sharing regimes. Most notably, the European Union has engaged in unilateral pressure to push states to modify their intelligence sharing practices and adopt greater privacy rights protections. The European Union has most actively imported privacy requirements onto other countries' intelligence gathering practices. Taking action in the name of international human rights, European Courts have led the effort to institute intelligence-sharing safeguards consistent with its interpretation of European human rights obligations. Europe's extraterritorial privacy governance has not been limited to national security practices, but has rather been part of a larger effort to govern global privacy law.[127] As legal scholars Jack Goldsmith and Tim Wu recognize, "For many purposes, the European Union is today the effective sovereign of global privacy law."[128] While European Courts have seized control of the EU's

---

[127] Canada has undertaken similar efforts more recently, but its actions have not had the same effect. For example, the Canadian Supreme Court also ordered Google to erase search results worldwide associated with a regarding an accusation of misappropriating confidential information and trade secrets. *See* Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, ¶3, https://scc-csc.lexum.com/scc-csc/scc-csc/en/16701/1/document.do; *see also* Jacob Gershman, *Judge Rules Canada Can't Make Google Delete Search Results in U.S.*, WALL ST. J. (Nov. 3, 2017), https://www.wsj.com/articles/judge-rules-canada-cant-make-google-delete-search-results-in-u-s-1509745395. A U.S court rejected the attempt to apply the Canadian ruling to U.S. jurisdiction. Google LLC v. Equustek Sols. Inc., 2017 WL 5000834, at *4 (N.D. Cal. Nov. 2, 2017) ("By forcing intermediaries to remove links to third-party material, the Canadian order . . . threatens free speech on the global internet."). As one analyst explains, this decision suggests that countries will not succeed in extraterritorial enforcement in the United States. Gershman, *supra.*

[128] *See* Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World*, 126 HARV. L. REV. 1966, (2006). *See also* Paul M. Schwartz, *The EU-U.S. Privacy*

privacy exportation, many of the European Union member states would like to strike a different balance—especially in the intelligence sphere.[129]

In recent years, the Court of Justice of the European Union (CJEU) has increasingly expanded its authority to review Member States' national security activity. In particular, the CJEU has actively policed data sharing practices for national security purposes, thereby influencing the security tradeoff for both the EU member states and also EU national security partners. The primary barrier of cross-border influence lies in CJEU's commitment to enforcing "an adequate level of protection" [130] for data transfers beyond the

---

Collision: A Turn to Institutions and Procedures, 126 HARV. L. REV. 1966, 1966 (2013) ("The EU has played a major role in international decisions involving information privacy, a role that has been bolstered by the authority of EU member states to block data transfers to third party nations, including the United States."); Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 77 (2012) (stating, in relevant part, that "something reasonably described as 'European standard' data privacy laws are becoming the norm in most parts of the world.").

[129] Privacy watchdog Privacy International has reported inconsistencies between EU member state practice and CJEU decisions. For example, as of July 2017, *zero* EU member states had adjusted their data retention practices or surveillance laws into compliance consistent with the 2016 CJEU *Watson* decision. *See National Data Retention Laws Since the CJEU's Tele-2/Watson Judgment*, PRIVACY INT'L (Sept. 2017), https://privacyinternational.org/sites/default/files/Data%20Retention_2017.pdf. Analysts have also noted that the UK's departure from the European Union was motivated at least in part by its antipathy towards the CJEU. *See, e.g.*, Elizabeth Piper, *Britain Outlines Plans To Break Free of European Court*, BUS. INSIDER (Aug. 22, 2017), http://www.businessinsider.com/r-britain-outlines-plans-to-break-free-of-european-court-after-brexit-2017-8 ("The European court, or ECJ, is hated by many pro-Brexit lawmakers in May's governing Conservative Party, who say it has slowly sucked power from British courts and parliament."). While the UK currently remains a European Union member state, it has reiterated its position on the CJEU's limited jurisdiction during the introduction of its recent data protection bill. According to the UK government, "National security is outside the scope of EU law. Consequently, the processing of personal data for national security purposes is not within scope of the GDPR or the Law Enforcement Directive ("LED")." Home Office, *Data Protection Bill: Factsheet—National Security Data Processing*, DEP'T DIGITAL, CULTURE, MEDIA & SPORT, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644829/2017-09-13_Factsheet04_national_security__1_.pdf.

[130] Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the

EU, even when it blends into the sphere of national security. In *Schrems v. Data Protection Commissioner* (Case C-362/14), the CJEU invalidated the transatlantic Safe Harbor agreement allowing for personal data sharing between European Union member states and the United States.[131] The CJEU overruled the Irish Data Protection Commissioner and found that in light of the Snowden revelations, the United States did not provide "adequate" protection to the personal data of E.U. citizens under the Safe Harbor framework.[132] In rejecting the 15-year old agreement that governed the data transfers for over 4,500 companies,[133] the CJEU pronounced that its preferred tradeoff balance must govern both the European Union, and the United States. The CJEU held:

> The right to respect for private life, guaranteed by Article 7 of the Charter and by the core values common to the traditions of the Member States, would be rendered meaningless if the State authorities were authorised to access electronic communications on a casual and generalised basis without any objective justification based on considerations of national security or the prevention of crime that are specific to the individual concerned and without those practices being accompanied by appropriate and verifiable safeguards.[134]

The CJEU asserted its ability to review the validity of national security interests as essential to accomplishing its mission to protect other human rights that fell within its jurisdiction. However, as expanded upon *infra*, the CJEU operates off an implicit assumption that human rights operate

---

Free Movement of Such Data, art. 45 (Jan. 25, 2012), http://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN [http://perma.cc/4ZY8-82A4.

[131] Robert Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, N.Y. TIMES (Oct. 9, 2015), http://www.nytimes.com/2015/10/11/business/international/behind-the-european-privacy-ruling-thats-confounding-silicon-valley.html.

[132] Case C-362/14, Schrems v. Data Prot. Comm'r, 2005 E.C.R. I-627, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

[133] Natalia Drozdiak & Sam Schechner, *EU Court Says Data-Transfer Pact With U.S. Violates Privacy*, WALL STREET J., (Oct. 6, 2015 1:42 P.M.), https://www.wsj.com/articles/eu-court-strikes-down-trans-atlantic-safe-harbor-data-transfer-pact-1444121361.

[134] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. I-31–32.

unilaterally in the privacy security tradeoff.[135] It also assumes the CJEU's right to give precedence to the CJEU's preferred balance point vis-à-vis other sovereign states. This assumption seemingly contradicts the CJEU's explicit finding that

> In a democratic society, a balance must be struck between these competing concerns, interests and values. Not every State will strike the same balance. One will place a greater emphasis on the right to privacy and one will place a greater emphasis on the requirements of national security. *It is important to state that it is not the function of this court to assess, still less resolve, the relative merits of these positions.*[136]

In light of the CJEU's stated position on the limited roles of the courts, the Court's decision was quite remarkable. Nevertheless, CJEU's resolution of "the relative merits of these [privacy tradeoff] positions" has created tensions with the privacy-security balances employed in other states' intelligence practices.

In addition to direct judicial review of national security data sharing arrangements, the European Union has also conditioned cross-border data sharing on its review of, among other factors, a non-EU country's national security practices.[137] Thus far, Andorra, Argentina, the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay have received adequacy decisions,[138] and both Canada and the

---

[135] *See* discussion *infra* Part IV.

[136] Case 2016 No. 4809 P., Data Prot. Comm'r v. Facebook Ireland Limited & Maximillian Schrems, §47 (Oct. 3, 2017), http://www.europe-v-facebook.org/sh2/HCJ.pdf (emphasis added).

[137] *See* Resolution of 6 April 2017 on the adequacy of the protection afforded by the EU-U.S. Privacy Shield, EUR. PARL. DOC. 2016/3018 ¶ 20 (RSP), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0131+0+DOC+PDF+V0//EN. Interview with Iain Bourne, Group Manager – Parliamentary and Government Affairs Department, United Kingdom Information Commissioner's Office (Aug. 1, 2017) (notes on file with author).

[138] European Union Comm.: 3rd Report of Session 2017–19, *Brexit: The EU Data Protection Package*, HOUSE OF LORDS §67 (2017) https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/7.pdf; *see also Adequacy of the Protection of Personal Data in non-EU Countries,* EUROPEAN COMM., https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en; HM GOV'T, *supra* note 65, at ¶ 37.

United States have received "partial" adequacy decisions.[139] By leveraging the stick of forbidding corporate-to-corporate cross-border information sharing, the CJEU has been able to exercise a powerful *de facto* influence on U.S. intelligence practices, and a significant barrier to intelligence sharing to the extent that the U.S. refuses to amend its practices.[140] As one European legal scholar described this success, "It is no exaggeration to state that in future, transnational privacy law will not be written in Brussels, but in in Luxembourg."[141] For example, in order to achieve the new US-EU Privacy Shield agreement, the United States has assigned a State Department official to serve as an Ombudsperson charged with the role of serving as the point of contact for foreign governments to raise concerns regarding US signals intelligence activities.[142] The Ombudsperson also collaborates with independent oversight bodies in the US government like the Inspectors

---

[139] Canada has a partial adequacy with respect to only commercial organizations subject to the PIPED Act, and the United States has an adequacy decision for organizations certified under the Privacy Shield only. *Id.*

[140] Alexander Garrelfs, *GDPR Top Ten: #3 Extraterritorial Applicability Of The GDPR*, DELOITTE, Apr. 3, 2017, https://www2.deloitte.com/nl/nl/pages/risk/articles/gdpr-top-ten-3-extraterritorial-applicability-of-the-gdpr.html. Even if one were to contest that the regulations only apply to those operating in EU jurisdiction negate the extraterritorial reach, the de facto extraterritorial imposition still applies. *See, e.g.*, Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 78 (2000) ("Most importantly, once U.S. businesses adopt internal data privacy policies to avoid EU transfer restrictions, they subject themselves to potential FTC enforcement proceedings for failure to comply with proclaimed policies. In any case, it will be pragmatically difficult for businesses to employ two sets of data privacy practices, one for EU residents (providing for greater privacy protection) and one for U.S. residents (providing for less."). Thomas Wischmeyer, *Faraway, So Close!' – A Constitutional Perspective on Transatlantic Data Flow Regulation*, *in* OBAMA'S COURT: RECENT CHANGES IN U.S. CONSTITUTIONAL LAW IN TRANSATLANTIC PERSPECTIVE (Anna-Bettina Kaiser, Niels Petersen & Johannes Saurer eds.) 14 (2017), https://ssrn.com/abstract=2877548 ("Moreover, the CJEU's strict scrutiny standard from Schrems coupled with the extraterritorial scope of EU privacy law established in Google Spain amount to a de-facto implementation of EU law on non-EU actors, in particular private actors based in the U.S.").

[141] Wischmeyer, *supra* note 140.

[142] *EU - U.S. Privacy Shield Ombudsperson*, U.S. DEP'T STATE, https://www.state.gov/e/privacyshield/ombud.

General to ensure that appropriate safeguards and procedures are in place.[143] This Privacy Shield, a creature of compromise,[144] is now under attack as privacy activists hope to use litigation to further heighten U.S. intelligence safeguards.[145] As illustrated through the Privacy Shield example, European judicial oversight poses the challenge of holding foreign government intelligence agencies to a privacy-security tradeoff different than the one that they have traditionally chosen.[146]

However, the United States is not entirely blameless in this regard. The CJEU *Schrems* decision responded to the United States' jurisprudence on the Fourth Amendment's inapplicability to non-U.S. citizens located outside of United States territory.[147] The United States Supreme Court has ruled that the Fourth Amendment does not "restrain the actions of the Federal Government against aliens outside of the United States territory."[148] In other words, when

---

[143] *Id.*

[144] *See, e.g.*, Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1967 (2013) (arguing that privacy "policymaking has not been led exclusively by the EU, but has been a collaborative effort marked by accommodation and compromise."); Maria Tzanou, *The War against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security*, 31 UTRECHT J. INT'L & EUR. L. 87 (2015) (arguing that EU-US privacy agreement might not actually have the privacy forcing effect on the United States that many analysts suggest).

[145] *Second Legal Challenge Launched Against "Privacy Shield"*, ELECTRONIC PRIVACY INFO. CENTER, Nov. 3, 2016, https://epic.org/2016/11/second-legal-challenge-launche.html.

[146] However, these changes in privacy-security balance may have thus far been mostly cosmetic. Maria Tzanou's assessment of EU data sharing agreements with the U.S. suggest that in practice, the United States has drawn the EU towards the security end of the privacy-security tradeoff without conceding any security powers. Tzanou, *supra* note 144, at 95 ("While potential 'spillovers of privacy' are not visible yet, 'spillovers of security' looking in the opposite direction, are certainly here.").

[147] *See generally* Wischmeyer, *supra* note 140, at 4.

[148] United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990). One must however note the irony that the justification for the decision rested in part on a need for international comity: "For better or for worse, we live in a world of nation-states in which our Government must be able to "functio[n] effectively in the company of sovereign nations." . . . Some who violate our laws may live outside our borders under a regime quite different from that which obtains in this country. Situations threatening to important American interests may arise half-way around the globe, situations which . . . [require cooperation] through diplomatic understanding, treaty, or legislation." *Id.*

it comes to foreign nationals located abroad, the United States' privacy-security tradeoff determines that for intelligence purposes, foreigners do not receive any privacy protection. This lack of constitutional procedural protection has culminated in foreign opposition to United States' Upstream surveillance practices authorized under Section 702 of the FISA Amendment Act of 2008.[149] The Amendment eliminated the previous statutory warrant and probable cause requirements for the collection of electronic communication by non-United States persons located extraterritorially.[150] The § 702 standard requires joint authorization by the Attorney General and the Director of the National Intelligence with a showing that the targets are "reasonably believed to be located outside the United States to acquire foreign intelligence information."[151] The Upstream collection physically taps the fiber-optic cables responsible for data traffic, and enables bulk communication interception.[152]

---

at 275. *See also* Wischmeyer , *supra* note 140, at 7 (discussing *Verdugo-Urquidez* effects); *see* discussion *supra* note 96 (detailing recent §702 jurisprudence).

[149] Daskal, *supra* note 62, at 346.

[150] *Id.* In contrast, the Act retains explicit due process safeguards for United States citizens. *See* Matt Olsen, *"Fixes" to Surveillance Law Could Severely Harm FBI National Security Investigations*, JUST SEC. (Nov. 27, 2017), https://www.justsecurity.org/47349/section-702-privacy-surveillance-law-severely-harm-fbi-national-security-investigations. However, there are still concerns of incidental collection of U.S. persons' communications. *See* Elizabeth Goitein, *Closing Section 702's Front-Door Search Loophole: A Critical Protection for Americans*, JUST SEC. (Oct. 24, 2017), https://www.justsecurity.org/46239/closing-section-702s-front-door-search-loophole-critical-protection-americans. Additionally, the Open Technology Institute has carefully documented the public record of FISA Section 702 compliance violations. Robyn Greene, *A History of FISA Section 702 Compliance Violations*, NEW AM.: OPEN TECH. INST. (Sep. 28, 2017), https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/#. *But see* PRIVACY & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 2 (2014), https://www.pclob.gov/library/702-Report.pdf (providing, in relevant part, that "[o]peration of the Section 702 program has been subject to judicial oversight and extensive internal supervision, and the Board has found no evidence of intentional abuse.").

[151] Daskal, *supra* note 62, at 346.

[152] Scarlet Kim, *How Bulk Interception Works*, PRIVACY INT'L (Sep. 30, 2016), https://medium.com/privacy-international/how-bulk-interception-works-d645440ff6bd; *see also* Daskal, *supra* note 62, at 349 ("Whereas collection through the PRISM program is done with the assistance of the ISP or phone service providers with

While in the past, Upstream collection included "to, from or about" information about a Section 702 Selector, beginning in May 2017, the Upstream collection only intercepted "to or from" communication data.[153] This interception capability takes advantage of the United States' domestic access control over Internet infrastructure,[154] and may set a precedential model for other states to engage in similar fiber-optics tapping practices.[155] Of note, despite the CJEU's condemnation of U.S. intelligence gathering practices, it is not clear that European governments provide greater safeguards against foreign government surveillance.[156] Other practices notwithstanding, the balance struck by U.S. government surveillance plays an outsized role given the effective control that U.S. companies exert over vast swaths of the Internet.[157] When the United States intelligence agencies need information,

---

whom the target interacts, "upstream" collection is done with the assistance of the Internet and telecommunications companies that control the fiber-optic cables over which a target's communications travel."); Ashley Gorski & Patrick Toomey, *Unprecedented and Unlawful: The NSA's 'Upstream' Surveillance*, AM. C.L. UNION (Sep. 23, 2016), https://www.aclu.org/blog/national-security/privacy-and-surveillance/unprecedented-and-unlawful-nsas-upstream (describing Upstream and accompanying concerns).

[153] *NSA Stops Certain Section 702 "Upstream" Activities*, NAT'L SEC. AGENCY: CENTRAL SEC. SERV., Apr. 28, 2017, https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.

[154] *See* Kim, *supra* note 152 ("The geographic location of the US features a high concentration of cables emanating from its east and west coasts."); Ian Brown, *The Feasibility Of Transatlantic Privacy-Protective Standards For Surveillance*, 23 INT'L J. L. & INFO. TECH. 23, 29 (2014), https://academic.oup.com/ijlit/article/23/1/23/2907405 ("USA is reluctant to accept limitations on its abilities to monitor data and communications relating to non-US persons that physically transit US territory—which NSA Director Keith Alexander has called a huge 'home-field advantage'.").

[155] *See* Daskal, *supra* note 50, at 474 ("The approach taken by the United States is likely to become a model for others, thus providing the United States a unique opportunity to set the standards.").

[156] *See* Schulhofer, *supra* note 51, at 250; *see also* Deeks, *supra* note 51, at 332 (detailing bulk collection practices in the United Kingdom, Germany, Sweden, and France).

[157] Daskal, *supra* note 50, at 474 ("While the problem of cross-border access to data is inherently international, the United States has an outsized role to play, given a combination of the U.S.-based provider dominance of the market"); Rubinstein et al., *supra* note 30, at 118 (stating, in relevant part, that "[t]he USA is perceived as having unique advantages in [transborder surveillance].").

they can (with the appropriate domestic safeguards) utilize the information in question. As viewed by non-Americans, U.S. hegemony over Internet services allows for intrusions by the United States government, irrespective of domestic national privacy protections.[158] While the United States has stated that it is undeterred by the possible consequences of its unchecked § 702 collection,[159] in practice, the US has taken steps to regulate its collection of foreign intelligence to account for privacy interests of those located abroad.[160]

---

[158] *See, e.g.*, Brief for Appellate at 8, In the Matter of A Warrant To Search A Certain E-Mail Account Controlled & Maintained By Microsoft Corporation. Microsoft Corp. v. United States (2014) (No. 14-2985-cv.), 2014 WL 7277561, at *8 ("European citizens are highly sensitive to the differences between European and U.S. standards on data protection. Such concerns are frequently raised in relation to the regulation of cross-border data flows and the mass-processing of data by U.S. technology companies. The successful execution of the warrant at issue in this case would extend the scope of this anxiety to a sizeable majority of the data held in the world's datacenters outside the U.S. (most of which are controlled by U.S. corporations) and would thus undermine the protections of the EU data protection regime, even for data belonging to an EU citizen and stored in an EU country."). *See also* Farhad Manjoo, *Why The World Is Drawing Battle Lines Against American Tech Giants*, N.Y. TIMES (Jun. 1, 2016), https://www.nytimes.com/2016/06/02/technology/why-the-world-is-drawing-battle-lines-against-american-tech-giants.html; *Internet Firms Face A Global Techlash*, ECONOMIST (Aug. 10, 2017), https://www.economist.com/news/international/21726072-though-big-tech-firms-are-thriving-they-are-facing-more-scrutiny-ever-internet-firms ("Some governments are unsettled by the growing role in their national lives of firms whose values are distinctively American, in particular in their commitment to free speech ahead of privacy.").

[159] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1130 (2017), https://review.law.stanford.edu/wp-content/uploads/sites/3/2017/04/69-Stan-L-Rev-1075.pdf ("[T]he [U.S. Department of Justice] has made it clear that it intends to use hacking techniques for all crimes, regardless of the potential cross-border implications."). In late 2017 and early 2018, § 702 underwent a heated reauthorization debate in the USA Liberty Act. *See, e.g.*, Olsen, *supra* note 150 (defending "national security imperative" for full reauthorization). In January 2018, Congress reauthorized FISA Section 702 for another six years. Ted Barrett & Ashley Killough, *Senate Passed FISA Section 702 Reauthorization*, CNN (Jan. 18, 2018), https://www.cnn.com/2018/01/18/politics/fisa-reauthorization-senate-vote.

[160] President Obama's Presidential Policy Directive 28 added additional safeguards for non-U.S. citizens located abroad and required that "signals intelligence activities must take into account that all persons should be treated with dignity and respect[.]" *See* PPD-28, *supra* note 96. *But see* Eric Manpearl, *The Privacy Rights of Non-U.S. Persons*

In short, the European Courts have taken steps to govern the intelligence sharing practices of not only the European Union Member States, but also their intelligence partners. This jurisprudence catches other states in a bind; states have their historical privacy-security tradeoff on one hand, and a legitimate need to engage in intelligence sharing with EU member states as well. Moreover, the United States' lack of extraterritorial privacy protection has further aggravated these barriers to intelligence sharing. The United States' legal stance, that the privacy-security considerations grant *no* privacy protections to foreigners located abroad, has generated understandable discomfort among partnering countries. In particular, foreign onlookers fear that the dissonance between domestic and foreign surveillance protections can facilitate a "revolving door" method by which their own intelligence services may partner with the United States to circumvent national limitations on domestic surveillance.[161]

The EU Court's approach to intelligence governance leads the EU to strike a particular privacy-security tradeoff for cross-border intelligence sharing. Privacy rights do not dissolve in the face of security; as the famous quote attributed to Benjamin Franklin goes, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."[162] However, the human rights interests weigh on both sides of the scale—too much privacy jeopardizes the human right to life and security. The European Courts have approached intelligence sharing with a privacy idealism that has infused their jurisprudence, but has met practical resistance by security apparatuses, including within EU member states.[163] Unless

---

in Signals Intelligence, 29 FL. J. INT'L L. 303 (2017) https://heinonline.org/HOL/P?h=hein.journals/fjil29&i=323 (arguing that "the United States should rescind PPD-28's expansion of privacy protections to non-U.S. persons because of its cost to U.S. intelligence capabilities, which are critical to protecting U.S. national security interests, the American people, and the U.S. Homeland.").

[161] *See, e.g.*, Kim et al., *supra* note 8.

[162] Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor, in* VOTES AND PROCEEDINGS OF THE HOUSE OF REPRESENTATIVES, 1755-1756 (1756), http://franklinpapers.org/franklin/framedVolumes.jsp?vol=6&page=238a.

[163] *See, e.g.*, Lorna Woods, *Transferring Personal Data Outside the EU: Clarification from the ECJ?*, EU L. ANALYSIS (Aug. 4, 2017), http://eulawanalysis.blogspot.com/2017/08/transferring-personal-data-outside-eu.html; *New Privacy International report shows that*

European law enforcement and intelligence partners comport with the requisite privacy data collection and data sharing standards, Europe may not be able to lawfully access or utilize the proffered foreign intelligence. As such, this standard has the potential to undermine Europe's effectiveness in receiving foreign information. It also undermines the national security of European partners who may no longer have the ability to share European intelligence.[164] Below, this Article tackles the challenge of designing criteria by which states may share intelligence with agencies that may strike a different privacy balance yet still ensuring the legitimate safeguarding of privacy interests.

V. ADOPTING CRITERIA FOR GOVERNMENT INTELLIGENCE SHARING

A. *International Law Governing Intelligence Sharing*

As Professor Ashley Deeks recognizes, when it comes to international law and the intelligence landscape, "few guideposts exist on how to proceed."[165] Professor Michael Reisman and James Baker have suggested that "the legality of any proactive covert operation should be tested by whether it promotes the basic policy objectives of the Charter, for example, self-determination; whether it adds to or detracts from minimum world order; whether it is consistent with contingencies authorizing the overt use of force; and whether covert coercion was implemented only after plausibly less coercive measures

---

21 European countries are unlawfully retaining personal data, PRIVACY INT'L (Oct. 23, 2017), https://www.privacyinternational.org/press-release/52/new-privacy-international-report-shows-21-european-countries-are-unlawfully; Schulhofer, *supra* note 51, at 253 (noting that the European Council of Ministers have spent years resisting "efforts to put EU privacy-protective legislation on a firmer footing.").

[164] Assuming that leaving the threat to national security unchecked is not a viable option, then the absence of foreign intelligence sharing will likely lead to increased surveillance of foreigners by European governments.

[165] Deeks, *supra* note 63, at 667. *See also* BORN ET AL., *supra* note 4, at 70 (stating that "relatively few countries have legislation on strategic surveillance and the jurisprudence of international courts is sparse.").

were tried."[166] Reisman and Baker's operational approach, while practically oriented, has received criticism for granting almost "unfettered discretion" to the state analyzing the issue.[167]

Some legal scholars have sought to find an international human right to privacy in the International Covenant on Civil and Political Rights (ICCPR), an international treaty with 169 parties.[168] Article 2(1) of the ICCPR requires: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[169] However, the United States has consistently taken the position that the ICCPR does not apply extraterritorially,[170] and state practice demonstrates "few, if any" extraterritorial privacy protections against intelligence surveillance.[171] As Asaf Lubin notes: "Despite this prevalent state practice, U.N. experts, human rights treaty bodies, and privacy NGOs have been adamant about protecting the myth of a singular and universal right to privacy. By doing so, they seem to 'abet the deception, avoiding the truth like someone pulling blankets over his head to avoid the cold reality of dawn.'"[172] Other scholars have identified

---

[166] W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW 26–27 (1992).

[167] Deeks, *supra* note 63, at 668.

[168] International Covenant on Civil and Political Rights, Dec. 19, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR], https://treaties.un.org/doc/Treaties/1976/03/19760323%2006-17%20AM/Ch_IV_04.pdf.

[169] *Id.* at art. 2, ¶ 1.

[170] *See, e.g.*, U.N. Hum. Rts. Comm., 53d Sess., 1405th mtg., ¶ 20, U.N. Doc. CCPR/C/SR.1405 (Mar. 31, 1995) (statement of Conrad Harper, Legal Advisor, U.S. Dep't of State) ("The Covenant was not regarded as having extraterritorial application. . . . During the negotiating history, the words 'within its territory' had been debated and were added by vote, with the clear understanding that such wording would limit the obligations to within a Party's territory.").

[171] Lubin, *supra* note 51, at 551.

[172] *Id.* at 515 (citing W. Michael Reisman, *Myth System and Operational Code*, 3 YALE STUD. WORLD PUB. ORD. 229, 237 (1977)). To take a few recent examples, *see, e.g.*, ANA VANESSA MIRANDA ANTUNES DA SILVA, ENHANCING SURVEILLANCE THROUGH THE

that even if one accepts that the ICCPR has extraterritorial effect, Article 17 of the ICCPR does not create an absolute limitation on intrusion, but rather only forbids "arbitrary or unlawful interference."[173] As a result, despite the ardent advocacy, most scholars agree that as a practical matter, United States opposition and state practice do not provide a viable implementation of universal privacy rights on the basis of the ICCPR.[174]

PATRIOT ACT AND THE FOREIGN INTELLIGENCE SURVEILLANCE AMENDMENT ACT, AND THEIR IMPACT ON CIVIL LIBERTIES: CAN HUMAN SECURITY BE COMPROMISED BY SECURITIZATION? 138 (2014), https://repositorium.sdum.uminho.pt/bitstream/1822/33875/1/Ana%20Vanessa%20Miranda%20Antunes%20da%20Silva.pdf ("[T]here is an increasing perception, not only but particularly in the EU, that the international human rights law applies extraterritorially and should be respected in order to abide by these international obligations."); Bignami & Resta, *supra* note 97, at 1 ("[Privacy] is a fundamental right enjoyed by all members of the human community and deserving of respect by all states whenever they act on their territory or enjoy "effective control" over persons."); Eliza Watt, *The Right To Privacy And The Future Of Mass Surveillance*, 21 INT'L J. HUM. RTS. 773, 776 (2017) ("Article 17 ICCPR and Article 8 ECHR apply extraterritorially, which means that states must respect the right to privacy whenever individuals are within their territory as well as their jurisdiction."). The U.N. General Assembly also adopted consensus resolution, G.A. Res. 68/167, ¶ 3 (Dec. 18, 2013), which "[a]ffirms that the same rights that people have offline must also be protected online, including the right to privacy." However, the U.S., which joined the resolution, issued an explanation reiterating that the ICCPR does not apply extraterritorially. U.S. Envoy at U.N., Explanation of Position on Draft Resolution L.26/Rev. 1 The Right to Privacy in the Digital Age (Nov. 25, 2014) (cited in Deeks, *supra* note 51, at 334).

[173] ICCPR, *supra* note 168, at art. 17. *See also* Bignami & Resta, *supra* note 97, at 6 ("The wording of Article 17 of the ICCPR makes clear that privacy is only protected against "unlawful" and "arbitrary" interferences."); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2138 (2014), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4980&context=flr ("This Article takes a middle ground that acknowledges that the United States has an extraterritorial duty under Article 2(1) to "respect" ICCPR rights including privacy, but then construes Article 17's prohibition on arbitrary interference narrowly to permit NSA surveillance abroad, given the legal constraints already in place governing the NSA's efforts."); Deeks, *supra* note 51, at 307 ("The Commentary to the ICCPR does indicate, however, that when states were negotiating Article 17, they understood the prohibition on "unlawful" or "arbitrary" interference to refer to acts that conflicted with the state's domestic legal system (which tends to run with the state's territory).").

[174] *See* Schulhofer, *supra* note 51, at 254 ("For these reasons, privacy advocates are right not to place all hopes on the broad jurisprudence of international human rights.")

International law governing state sovereignty might also seem to prevent foreign intelligence collection and its subsequent sharing. As Bert-Jaaps Koop and Morag Goodwin contend,

> In the strict—and still dominant—interpretation of international law, any evidence-gathering activity in a foreign state, including the making of a mere phone call, can be considered a breach of state sovereignty. Accessing data that is, or later turns out to be, stored on a server located in the territory of another state, without the prior consent of that state, constitutes a breach of the territorial integrity of that state and thus a wrongful act.[175]

In other words, according to Koop and Goodwin, non-consensual intelligence gathering violates the international legal principle of state territorial integrity. The authors point to Article 19 of the Cybercrime Convention, which provides that extended computer network searches should not cross national borders in the absence of two circumstances outlined in Article 32: a) lawful and voluntary consent from foreign actors, or b) if the targeted information is publicly available.[176] If states violated international law in collecting shared intelligence, then one might consider international law to forbid any subsequent use of the information.

Koops and Goodwin's point notwithstanding, further case law developed by the rights-protective European Court of Human Rights may have cabined the effect of international law limitations for cross-border computer searches. In *Weber and Saravia v. Germany*, the Plaintiffs charged Germany's Federal Intelligence Service (*Bundesnachrichtendienst*) with the interception of telecommunications and the subsequent use of personal data.[177] The Court took important notice of the fact that while the data may have been relayed from foreign countries, the devices used to monitor the wireless

---

[175] Koops & Goodwin, *supra* note 32, at 9.

[176] *Id.* at 53 (citing Convention on Cybercrime, Nov. 23, 2001, C.E.T.S. 185). A similar provision is included in article 40 of the League of Arab States' Arab Convention on Combating Information Technology Offences (available at https://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd).

[177] Weber & Saravia v. Germany, App No 54934/00, 2006-XI [2006] Eur. Ct. H.R. 1173, Admissibility (2006), http://hudoc.echr.coe.int/webservices/content/pdf/001-76586.

communications were situated in sovereign German territory.[178] In doing so, the Court held that this German interception did not constitute conduct "which interfered with the territorial sovereignty of foreign States as protected in public international law."[179] Under parallel reasoning, a state would not interfere with the territorial sovereignty of any foreign state as long as that state accessed the wireless Internet data from a computer located in its own country. Additionally, in contrast to criminal evidence collection, foreign intelligence gathering constitutes acts of espionage. When it comes to espionage,

> one can identify scores of sources in international law to establish the existence of the *Jus Ad Explorationem* (the Right to Spy). So much so, in fact, that "to claim that espionage is not a priori permissible as a sovereign prerogative is simply inconceivable in our public world order" and certainly in discontent with both vast bodies law and practice.[180]

As such, state sovereignty does not provide a barrier to intelligence gathering under international law. Therefore, the subsequent intelligence sharing does not constitute 'fruit of the poisonous tree.'

Finally, at least one court—the European Court of Human Rights—has tied the international law principles governing surveillance and intelligence gathering to intelligence sharing. In *Liberty v UK*, the ECtHR held that the privacy safeguards on intelligence data must detail the "procedure to be followed for selecting for examination, *sharing*, storing and destroying intercepted material."[181] In the absence of conflicting jurisprudence, the ECtHR case law makes a plausible contention that any international law

---

[178] *Id.* at ¶ 86 ("The Court observes that the impugned provisions of the amended G 10 Act authorise the monitoring of international wireless telecommunications, that is, telecommunications which are not effected via fixed telephone lines but, for example, via satellite or radio relay links, and the use of data thus obtained. Signals emitted from foreign countries are monitored by interception sites situated on German soil and the data collected are used in Germany.").

[179] *Id.*

[180] Asaf Lubin, *The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum*, 57 WASHBURN L. J. 17, 56 (2018).

[181] Liberty v. United Kingdom, App. No. 58243/00, Eur. Ct. H.R., Judgment (July 1, 2008), § 69, http://hudoc.echr.coe.int/eng?i=001-87207 (emphasis added).

governing intelligence collection mandates some privacy consideration in intra-governmental intelligence sharing.

B. *Scholarship on Intelligence Governance Frameworks*

The legal field has proliferated substantial writing on international intelligence bodies and covert operations, but far less attention has been paid to intelligence sharing. Some of the classic literature recognizes the importance of data sharing but does not address the challenges arising from various privacy regimes. For example, work by Professors Myres McDougal, Harold Lasswell and Michael Reisman note the importance of intelligence sharing across governments: "The model of Interpol may be simulated by 'Interspy,' a service that draws upon the sources available to all organizations willing and able to work together to expose threats to world public order."[182] While McDougal *et al* recognize the importance of intelligence sharing,[183] they do not address the differences in privacy-security balances.[184] Over the past few decades, with what Professor Margo Schlanger has recognized a rise of "intelligence legalism," legal scholarship has taken a renewed interest between law and the intelligence community.[185] Much of the effort has focused on MLAT reform, which grapples with the more circumscribed problem of obstruction in law enforcement data sharing requests.[186] Other

---

[182] McDougal et al., *supra* note 44, at 447.

[183] *Id.* at 422 ("As global interdependence increases, this imbalance will ultimately prove to be detrimental to planning on the part of even the most developed communities, and will give greater impetus to the sharing of processing technology.").

[184] *Id.*

[185] Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112, 113 (2015).

[186] *See* Jennifer Daskal & Andrew Keane Woods, *Cross-Border Data Requests: A Proposed Framework*, LAWFARE (Nov. 24, 2015, 8:00 AM), https://www.lawfareblog.com/cross-border-data-requests-proposed-framework; *see also* Daskal, *supra* note 50; Daskal, *supra* note 62, at 393 ("these concerns highlight the need for new cross-border mechanisms that facilitate law enforcement access to data, yet also respect the sovereign interest in setting privacy protections and controlling law enforcement operations within one's jurisdiction."); ANDREW K. WOODS, DATA BEYOND BORDERS: MUTUAL LEGAL ASSISTANCE IN THE INTERNET AGE (2015), https://globalnetworkinitiative.org/wp-content/uploads/2016/12/GNI-MLAT-Report.pdf; MICHAEL CHERTOFF & PAUL ROSENZWEIG, A PRIMER ON GLOBALLY

proposals tackle "government data collection" with a broad scope and do not clarify whether they intend their proposals to address the MLAT process or also include government intelligence sharing.[187]

Inter-governmental data-sharing regimes have been woefully under-theorized by the legal literature.[188] Nearly all the work focuses on domestic privacy governance over the home regime and does not seriously engage with the question of harmonizing the different privacy-security tradeoffs for intelligence sharing between allied governments. Instead, the goal is to regulate the surveillance practices of each country, so a uniform sharing

---

HARMONIZING INTERNET JURISDICTION AND REGULATIONS (Global Comm'n on Internet Gov., Paper No. 10 2015), https://www.cigionline.org/sites/default/files/gcig_paper_no10_0.pdf; Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance*, *in* BULK COLLECTION: SYSTEMATIC GOVERNMENT ACCESS TO PRIVATE-SECTOR DATA (Fred H. Cate & James X. Dempsey eds., 2017), http://dx.doi.org/10.2139/ssrn.2696163; Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. J. ONLINE (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age; Gail Kent, Sharing Investigation Specific Data with Law Enforcement—An International Approach (Feb. 14, 2014) (Stanford Pub. L. working paper), http://ssrn.com/abstract=2472413. For a useful overview of the current status of UK-UK MLAT negotiations as well as some of the remaining concerns, see Tiffany Lin & Mailyn Fidler, *Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement* (Berkman Klein Center Research Pub. No. 2017-7, 2017), https://ssrn.com/abstract=3035563.

[187] *See, e.g.*, Microsoft Corporate Blog, *Time For An International Convention On Government Access To Data*, MICROSOFT (Jan. 20, 2014), https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data (writing generally about "government access to data"). However, given Microsoft's well-documented challenges navigating conflicts over compelled data disclosures, see United States v. Microsoft Corp., SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp, one may reasonably assume that the Microsoft's principle concern centers on government access to data stored by private companies, not exchanged with foreign intelligence agencies.

[188] Rubinstein et al., *supra* note 30, at 105 ("Although most of the countries appear to consider multinational access and sharing essential to national security and law enforcement activities, these arrangements received relatively little attention in the papers that were commissioned. Overall, it seems, there has been relatively little discussion of the complex legal and political issues associated with asserting jurisdiction over data stored in other countries or relating to citizens of other countries.").

standard is often assumed. Professor Peter Margulies' article presents an exception to this rule; while Margulies does not consider intelligence sharing, he envisions complementarity providing procedural pluralism to legitimate differing state surveillance practices under international law.[189] More typical is the stance epitomized by Edward Snowden supporters, who have clamored for the introduction of a "Snowden Treaty," which calls to outlaw mass surveillance and create whistleblower protections.[190]

Some scholars and human rights groups have sought to forge limiting principles conjured from international human rights law. Rubinstein *et al* have sought to design a privacy framework directly based on the principles governing surveillance (for law enforcement and intelligence gathering) extrapolated from the European Court of Human Rights jurisprudence, [191] and suggest fourteen principles from the ECtHR.[192] However, the Rubinstein analysis does not directly consider intelligence sharing with foreign governments. Similarly, privacy activist group Necessary & Proportionate has outlined thirteen principles that they believe provide the international human rights law standards for government communications surveillance.[193] While at first blush, one of the principles, safeguards for international cooperation, seems to cover the subject of this inquiry—intelligence sharing, it entirely elides the issue. The principle discusses international cooperation within the context of MLATs. MLATs are used only for criminal

---

[189] Margulies, *supra* note 173, at 2157 ("A state could choose from a number of procedural options that would accomplish these goals, without being locked into specific measures that might not fit with that state's history or traditions. Procedural pluralism would also minimize conflicts with other international rules, such as the law of armed conflict and Security Council resolutions mandating counterterrorism efforts.").

[190] *What is the Snowden Treaty*, SNOWDEN TREATY, http://www.snowdentreaty.org; *The Snowden Treaty: A new International Treaty on the Right to Privacy, Protection Against Improper Surveillance and Protection of Whistleblowers*, SNOWDEN TREATY, http://media.wix.com/ugd/fb845b_89e20fe385844f348fbc79a6ede39a4d.pdf.

[191] Rubinstein et al., *supra* note 30, at 111.

[192] *Id.*

[193] *Necessary and Proportionate: International Principles On The Application Of Human Rights To Communications Surveillance*, NECESSARY & PROPORTIONATE COALITION (May 2014), https://necessaryandproportionate.org/principles.

investigations, and do not cover intelligence sharing.[194] It is possible that Necessary & Proportionate have implicitly adopted the position that intelligence sharing should fall within the MLAT framework, although this delivers a strained reading given MLATs' traditional scope. Finally, President Obama's Presidential Policy Directive 28 establishing voluntary minimum protections for foreigners during government intelligence activities has introduced another helpful framework, as the protections outlined in PPD-28 benefited from the insight of the real security needs that government intelligence seeks to address.[195] However, the PPD-28 framework is incomplete, both in its lack of legal discussion and lack of detail.

The few works that do directly consider inter-governmental intelligence sharing almost unfailingly adopt a tunnel vision towards only the "privacy" elements of the privacy-security tradeoff.[196] Take, for example, Eliza Watt's effort supporting the proposed Intelligence Codex for the Council of Europe.[197] David Cole and Federico Fabbrini argue for a comprehensive transatlantic privacy between the EU and US that would close the protection gap endemic in the lack of extraterritorial privacy protection under each jurisdiction.[198] Ian Brown *et al* undertakes the project to outline "privacy-conscious intelligence reform," and proposes a series of standards, but do not actually consider

---

[194] Greg Nojeim, *MLAT Reform: A Straw Man Proposal*, CTR. FOR DEMOCRACY & TECH. (Sep. 3, 2015), https://cdt.org/insight/mlat-reform-a-straw-man-proposal.

[195] PPD-28, *supra* note 96 (committing to 1) proportionality, 2) use, dissemination, and retention limitations 3) data security and accuracy protections 4) oversight procedures.).

[196] *See* Schulhofer, *supra* note 51, at 253 ("[T]he international law scholarship, even on its own terms, is often incomplete, because much of it is framed in terms applicable only to ordinary law enforcement, without taking on board the extra flexibility and secrecy that is arguably "necessary in a democratic society" in the case of surveillance for national security purposes.").

[197] Watt, *supra* note 172, at 784 ("There can be no doubt that a binding treaty, such as the proposed Codex, is necessary."). The Council of Europe suggested four principles to govern intra-European intelligence cooperation: 1) prohibition on mutual political and economic espionage; 2) foreign intelligence activity must receive *ex ante* approval from the target state; 3) prohibition on tracking, analyzing, or storing data without individualized suspicion from a friendly state, and 4) prohibition on compelled disclosures from telecommunication and internet companies without a court order. *Id.*

[198] Cole & Fabbrini, *supra* note 30, at 223.

intelligence-sharing.[199] Privacy International's recent call for greater transparency over government intelligence sharing reflects the renewed interest in bringing law into the shadowy sphere of government intelligence, but the privacy advocacy group does not suggest a framework for intelligence governance beyond public transparency.[200]

Professor Stephen Schulhofer rejects "the developing consensus" that a comprehensive multilateral agreement to abide by surveillance principles or minimum standards would help regulate expansive state surveillance activity.[201] Instead, Schulhofer argues that a "privacy-conscious international framework" would allow "the fox to design th[e] henhouse," and his "ultimate concern [] for privacy and democracy worldwide" leads him to reject an agreement that would almost inevitably lead to an arrangement at less than maximal privacy.[202] Instead, Schulhofer promotes bilateral commitment in which each party grants whichever safeguards it observes when engaging in surveillance over its own citizens.[203]

Schulhofer is right. A multinational arrangement would necessarily result in less privacy safeguards than required for national security activity in the maximally protective states. But from here we differ. Unlike Schulhofer, I reject the premise that privacy rights are the only rights at play here and

---

[199] Ian Brown et al., Towards Multilateral Standards for Surveillance Reform (Jan. 5, 2015) (Oxford Internet Institute Discussion Paper), https://ssrn.com/abstract=2551164 (outlining standards of 1) legitimate national security purposes for surveillance, 2) establishment of extraterritorial privacy standards, 3) tailored limitations on data collection beyond a broad "relevant to national security interest," 4) minimization standards, 5) methods of oversight, 6) protection against unauthorized access.). Their closest standard is "onward transmission/purpose limitation," but this limitation refers to alternative non-intelligence uses, not sharing with another intelligence agency. *See id.* at 5–6. The paper also provides an excellent recap of some of the existing intelligence reform proposals. *Id.* at 20–24.

[200] *Privacy International Launches International Campaign For Greater Transparency Around Secretive Intelligence Sharing Activities Between Governments*, PRIVACY INT'L (Oct. 23, 2017), https://www.privacyinternational.org/press-release/51/privacy-international-launches-international-campaign-greater-transparency-around.

[201] *See* Schulhofer, *supra* note 51, at 242.

[202] *Id.*

[203] *Id.* at 261.

contend that security considerations also implicate human rights in a way that justifies tailored departures for intelligence-sharing purposes. Security officials are not the "fox in the henhouse," but rather serious stakeholders in a privacy-security duet balancing competing human rights.

Ashley Deeks and Peter Margulies are possibly the only scholars who have employed a true balance-oriented approach in designing an intelligence-sharing framework.[204] However, both works only treat intelligence sharing as an incidental measure to a state's domestic intelligence program. Deeks recognizes that "[there is no] disagreement that the right to privacy is a qualified right, subject to lawful and non-arbitrary interference by a state."[205] Instead, she suggests six "procedural norms" that would create meaningful privacy protections without harming national security.[206] Deeks touches briefly on intelligence sharing by recognizing that a preference for domestic surveillance would help address the "revolving door" concern, and notes that such a principle "could increase the need for ongoing coordination among allies' intelligence agencies."[207] Similarly, Margulies offers a list of procedural protections.[208] Like Deeks, Margulies recognizes that harmonizing standards "could also remove any barriers to cooperation between the United States and foreign states."[209] This Article goes further in providing a cooperation

---

[204] Margulies, *supra* note 173, at 2157; Deeks, *supra* note 51, at 346.

[205] Deeks, *supra* note 51, at 305. This is not to say that other frameworks do not recognize that the privacy right is not absolute. To the contrary, they uniformly allow for privacy intrusions in some circumstances. However, what distinguishes Deeks' scholarship from the other works is an explicit recognition that the *goal* of the framework should not be to achieve the maximum privacy protections possible.

[206] Deeks, *supra* note 51, at 351–63 (the six procedural norms are 1) notice to public of applicable rules, 2) limits on the reasons for data collection and use, 3) requirement for periodic reviews, 4) limits on data retention, 5) preference for domestic surveillance, and 6) neutral oversight body).

[207] *Id.* at 366.

[208] Margulies, *supra* note 173, at 2157. Margulies' procedural protections include 1) notice about grounds for surveillance, 2) oversight of surveillance programs, 3) deterrence of arbitrary official conduct, including targeting of political opponents or disfavored ethnic, racial, or religious groups, and includes procedural flexibility for state implementation. *Id.*

[209] *Id.* at 2165.

framework tailored to a thorough and detailed exploration of inter-governmental intelligence sharing.

C. *Proposed Framework*

As noted *supra* in Part 0, widespread disagreement persists over the relevant international law governing intelligence sharing. This framework utilizes commonly cited principles of international law as a helpful starting point. Drawing on prior literature, I condense the fourteen international law principles of government surveillance identified by Necessary & Proportionate[210] into 5 primary categories: 1) principle of legality 2) principle of safeguarding against abuse 3) principle of proportionality 4) principle of transparency and oversight 5) principle of notification and remedies. In order to tailor this framework to the challenges of intelligence sharing, I include three additional considerations: 6) the principle of complementarity 7) the principle of good faith and 8) the exigency exception. Using this framework, I outline a way forward for governing intelligence sharing while respecting legitimate differences in countries' privacy-security balance.

In devising a framework for governmental intelligence sharing, one approach would be to adopt a highest common denominator and to use the same standards to govern intelligence sharing as are used for law enforcement sharing and other police activities. Some privacy rights advocates, including Privacy International, have opted for this approach.[211] Such individuals can point to American law, which grants the same Fourth Amendment privacy protection to American citizens, regardless of whether the surveillance arises in the context of petty crime or dire threats to national security.[212] As the U.S. Supreme Court famously held in the *Keith* case, a government's national security concerns "do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a

---

[210] *See* Rubinstein et al., *supra* note 30, at 104 (condensing the fourteen necessary and proportionate principles into thirteen categories).

[211] *See* Brown, *supra* note 154, at 23–25 (conflating intelligence and law enforcement privacy standards).

[212] *See infra* note 218.

search or surveillance."[213] However, as Professor Schulhofer notes, for many democratic countries, "such fundamental issues as the required level of suspicion, the role of suspect-specific judicial approval ex ante, and the degree to which transparency and oversight are relaxed in the national security context."[214]

There are good reasons for differentiating intelligence and law enforcement data collection. For example, intelligence purposes may fundamentally differ from those of law enforcement: "Intelligence often searches for new information, whereas law enforcement often looks for additional information."[215] This purposive difference reasonably leads to one to expect different evidentiary standards—"probable cause" often poses a prohibitively challenging standard when searching for new information. Therefore, this paper rejects the notion that the same criminal law enforcement information sharing standards should also apply to intelligence sharing.

"In the field of monitoring bilateral and multilateral intelligence sharing arrangements, there has been particular inadequacy of oversight."[216] Thus far, the European Court of Human Rights (ECtHR) has developed the most comprehensive case law on surveillance. However, as the Court's name suggests, the ECtHR "takes the community interest in the right to privacy and the corresponding state duty to respect that community obligation very seriously."[217] As such, it comes as little surprise that privacy advocates

---

[213] *See* United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div., 407 U.S. 297, 321 (1972) (holding government's national security concerns "do not justify departure in this case from the customary Fourth Amendment requirement of judicial approval prior to initiation of a search or surveillance.").

[214] Schulhofer, *supra* note 51, at 245 ("There is wide variation, even among Western democracies, on such fundamental issues as the required level of suspicion, the role of suspect-specific judicial approval *ex ante*, and the degree to which transparency and oversight are relaxed in the national security context.").

[215] Mailyn Fidler, *MLAT Reform: Some Thoughts From Civil Society*, LAWFARE (Sep. 11, 2015), https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society.

[216] Lubin, *supra* note 51, at 548.

[217] Bignami & Resta, *supra* note 97, at 2. Because the European Court of Human Rights (ECtHR) views privacy as a human right, its jurisprudence has found that "all persons are covered and are guaranteed the same treatment by the state." *Id.* As noted in Part VII.A, this interpretation is contested as a matter of international law.

campaign for the ECtHR as the privacy floor. The CJEU decision in *Kadi v. Commission* has provided ammunition for the "privacy floor" approach by establishing that "EU concepts on fundamental rights prevail, whenever this is necessary, over international law."[218]

Nevertheless, the ECtHR has developed its jurisprudence while leaving some room for discretion, and despite its privacy-protective orientation, many of the ECtHR privacy decisions have recognized the need for flexibility in the intelligence space.[219] For example, while the ECtHR has recognized "rather strict standards" governing the interception of communication, the Court has expressly recognized that those standards do not necessarily apply in other intelligence gathering contexts.[220] Furthermore, the European Court has taken the reasonable approach of recognizing the existence of tradeoffs, and has not perpetuated the mistaken notion that surveillance constitutes a per se violation of human rights.[221] Even Privacy International acknowledges that intelligence activities necessarily cannot operate with complete transparency over the scope and nature of government intelligence-sharing agreements.[222] While the ECtHR provides one possible approach, its institutional mission-

---

[218] Hielke Hijmans, *The European Union As Guardian of Internet Privacy: The Story of Art 16 TFEU*, 31 L. GOVERNANCE & TECH. SERIES 1, 473 (2016) https://link.springer.com/content/pdf/10.1007/978-3-319-34090-6.pdf.

[219] Respondent's Open Response, Privacy Int'l v. United Kingdom, Case No. IPT/13/92/CH, (Investigatory Powers Trib. 2014) (U.K.) and Liberty v. United Kingdom, Case No. IPT/13/77/H (Investigatory Powers Trib. 2014) (U.K.) [hereinafter UK IPT Response], https://www.liberty-human-rights.org.uk/sites/default/files/The%20Intelligence%20Services%20open%20response%20to%20Liberty%E2%80%99s%20and%20Privacy%20International%E2%80%99s%20claims%2015th%20November%202013.pdf.

[220] *Id.* (citing Uzun v. Germany (2011) 53 EHRR 24, at §66). *See also* McE v. Prison Service of Northern Ireland [2009] 1 AC 908, per Lord Carswell at § 85.

[221] Rubinstein et al., *supra* note 30, at 119.

[222] *Human Rights Implications of Intelligence Sharing*, PRIVACY INT'L 9 (2017), https://www.privacyinternational.org/sites/default/files/2017-12/PI%20Briefing%20to%20National%20Intelligence%20Oversight%20Bodies_12_Sept.pdf ("Privacy International specifically urges national intelligence oversight bodies, to the extent permitted under their mandates, to: make publicly available as much information as possible as to the nature and scope of intelligence sharing arrangements to which their governments are party, as well as the rules governing such arrangements[.]").

orientation leads to an uncompromising approach that does not accommodate the privacy-security balance adopted by most countries. In contrast, the framework below secures meaningful privacy protections while still preserving maximal respect for sovereign discretion.

i. Principle of Legality

A basic requirement for the rule of law is that rules must be based in law, with a degree of foreseeability and accessibility. This principle of legality is generally uncontroversial and considered a core principle of international law.[223] Intelligence-sharing arrangements should have these provisions to the extent reasonably practicable. It is true that political considerations may weigh in favor of preventing the public disclosure of intelligence cooperation with some countries,[224] but the principles by which governments conduct themselves in the intelligence-sharing process would not adversely affect their capacity to conduct their jobs. At the same time, such principles would also provide a circulated standard against which intelligence agencies, their counterparts, and oversight bodies could hold agency action accountable.

Both the United States and the EU agree that the ICCPR requires some respect for privacy rights of those under a country's domestic jurisdiction. Specifically, that states have an obligation to refrain from "arbitrary or unlawful interference" into the private lives of those under the state's domestic jurisdiction.[225] This principle of legality is expressed in the first clause of Article 8(2) of the European Convention on Human Rights, stating

---

[223] Beth Van Schaack, *The Principle of Legality in International Criminal Law*, 103 AM. SOC. OF INT'L L. 101, 101 (2009) ("The principle of *nullum crimen sine lege* is a fundamental principle of criminal law. It has particular resonance at the international level given the relative lack of clarity surrounding certain international legal norms.").

[224] *See generally* Ashley Deeks, *A (Qualified) Defense of Secret Agreements*, 49 Ariz. St. L.J. 713 (2017) http://arizonastatelawjournal.org/wp-content/uploads/2017/09/Deeks_Pub.pdf.

[225] Deeks, *supra* note 51, at 305 ("The United States, for example, believes that states may engage in surveillance that is in accordance with transparent laws and that furthers a legitimate aim. Human rights groups favor a higher standard drawn from ECtHR case law: The interference must be necessary in the circumstances of the case and proportional to the end sought, and the surveillance must be conducted under specific and clearly defined laws.").

that "[t]here shall be no interference by a public authority with the exercise of this right except such as is *in accordance with the law.*"[226] In other words, the exercised powers have some basis in domestic law and meet a foreseeability requirement.[227] Accordingly, secret rules without any basis in domestic legislation cannot be in accordance with the law for the purposes of restricting rights.[228] This 'accordance with the law' requirement poses a low standard; even broad delegations of power, such as those in the Chinese National Security Law,[229] have a basis in domestic law.[230] This delegation may be analogized to the broad "intelligible principle" requirement in American administrative law and is unlikely to carry significant substantive impact beyond public accessibility to the relevant law.[231]

However, the law must also enable a degree of foreseeability. This has led international privacy scholars to argue that privacy rights require that "[a]ny limitations to the right to privacy 'must be provided for by law, and the law must be sufficiently accessible, clear, and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.'"[232] As interpreted by the ECtHR, the essential test for foreseeability asks whether the laws sufficiently indicate the scope of discretion and the manner of exercise "to give the individual adequate protection against arbitrary interference."[233] However, the ECtHR highlights

---

[226] European Convention on Human Rights, *supra* note 25 (emphasis added).

[227] Brown et al., *supra* note 199.

[228] *Id.*

[229] *See supra* notes 124, 125.

[230] *But see* Szabó & Vissy v. Hungary, App. No. 37138/14, Eur. Ct. H.R., Judgment, ¶ 78 (2016), http://hudoc.echr.coe.int/eng?i=001-160020.

[231] *See* J.W. Hampton, Jr., & Co. v. United States, 276 U. S. 394, 409 ("If Congress shall lay down by legislative act an intelligible principle to which the person or body authorized to fix such rates is directed to conform, such legislative action is not a forbidden delegation of legislative power.").

[232] Lubin, *supra* note 51, at 542.

[233] Malone v United Kingdom, App. No. 8691/79, (1984) 7 Eur. H.R. Rep 14, §86. *See also* Weber & Saravia v. Germany, App No 54934/00, 2006-XI [2006] Eur. Ct. H.R. 1173, Admissibility, §§ 78–79 (2006), http://hudoc.echr.coe.int/webservices/content/pdf/001-76586 (the laws must be sufficiently detailed to give "an adequate indication" to the times and circumstances under which the government may engage in surveillance activities).

that the foreseeability requirement should not be taken to preclude effective surveillance: "the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly."[234] The UN High Commissioner for Human Rights (UNHCHR) has echoed the generally-accepted the legality requirement, interpreting surveillance carried out on the basis of a law to require (a) public accessibility and (b) sufficient precision for reasonable foreseeability of the consequences of certain conduct.[235]

In the intelligence-sharing context, applying the legality principle makes sense. States should have laws governing intelligence sharing. The U.N. Special Rapporteur on Counter-Terrorism and Human Rights has noted

> The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority. Information concerning an individual's communications may be shared with foreign intelligence agencies without the protection of any publicly accessible legal framework and without adequate (or any) safeguards . . .. Such practices make the operation of the surveillance regime unforeseeable for those affected by it.[236]

While security concerns may weigh in favor of limiting the disclosure of specific information sharing arrangements, laws delineating the general circumstances and procedures under which a government engages in intelligence sharing would allow "sufficient adequate protection against arbitrary interference" and offset concerns of unbridled government power to

---

[234] Malone v United Kingdom, App. No. 8691/79, (1984) 7 Eur. H.R. Rep 14, § 67. *See also* OFFICE OF THE SPECIAL RAPPORTEUR FOR FREEDOM OF EXPRESSION OF THE INTER-AMERICAN COMMISSION ON HUMAN RIGHTS, FREEDOM OF EXPRESSION AND THE INTERNET 75 (2013) ("The State must be transparent with respect to the laws regulating communications surveillance and the criteria used for their application. The principle of 'maximum disclosure' is applicable to this issue.").

[235] *See* Bignami & Resta, *supra* note 97. The UNHCHR elements also include (c) provisions ensuring legitimate aims and (d) effective safeguards against abuse, but (c) and (d) simply suggest a divergent taxonomy, as both concern safeguards against abuse addressed below.

[236] Lubin, *supra* note 51, at 548–49.

exchange private information without due consideration of individual privacy interests. Adopting public intelligence sharing standards would achieve this goal and provide the legally grounded governance standards expected in the international community.

Getting states to recognize the legality principle should prove relatively uncontroversial, and states' acceptance would not likely face ideological resistance. The difficulty arises at the implementation stage over which safeguards adequately ensure that the government does not engage in arbitrary or unlawful interference. For example, the United States believes that this limitation is satisfied as long as its surveillance is consistent with transparent laws and furthers a legitimate aim, whereas the ECtHR adds additional principles of necessity and proportionality.[237] The next section seeks to untangle the morass over what should count as sufficient safeguards against abuse.

ii. Principle of Safeguards against Abuse

The appropriate intelligence-sharing framework should delineate procedural requirements that safeguard against abuse. In order to fulfill the legality principle, countries sharing information should both have publically issued safeguarding procedures governing their intelligence practices. In *Weber and Saravia v. Germany*, the ECtHR helpfully identified six procedural safeguards to govern European communications interception:

> [1] the nature of the offences which may give rise to an interception order;
>
> [2] a definition of the categories of people liable to have their telephones tapped;
>
> [3] a limit on the duration of telephone tapping;

---

[237] Deeks, *supra* note 51, at 305–06 ("The United States, for example, believes that states may engage in surveillance that is in accordance with transparent laws and that furthers a legitimate aim. Human rights groups favor a higher standard drawn from . . . [ECtHR] case law: The interference must be necessary in the circumstances of the case and proportional to the end sought, and the surveillance must be conducted under specific and clearly defined laws.").

> [4] the procedure to be followed for examining, using and storing the data obtained;
>
> [5] the precautions to be taken when communicating the data to other parties;
>
> [6] and the circumstances in which recordings may or must be erased or the tapes destroyed[238]

For the purpose of intelligence sharing, Categories [1], [3], [4] and [5] are most important.

First, states should publically disclose the nature of the offenses and purposes that warrant intelligence sharing. Intelligence sharing should remain limited to exchanges of intelligence information for national security purposes and should not operate as a loophole for the transfer of other types of information. In order for the information to be shared through intelligence channels, the collected information should have been collected for security purposes. For example, the United States has committed to exclusively collecting signals intelligence for foreign intelligence or counterintelligence purposes to support national and departmental missions.[239] Intelligence sharing agreements should provide similar commitments to exclusive national security utilization among both the collecting and transferring parties. This is particularly important in light of concerns that signals intelligence may be utilized for the "purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[240] While states will differ on the extent to which these protected categories may factor into national security practices, establishing clear purposes for intelligence exchange facilitates effective oversight and provides clear normative guidelines for the state's intelligence apparatus. While Category [2] would help provide foreseeability to know the specific categories of individuals liable to have their information

---

[238] Lubin, *supra* note 51 (citing Weber & Saravia v. Germany, App No 54934/00, 2006-XI [2006] Eur. Ct. H.R. 1173, Admissibility, ¶ 95 (2006), http://hudoc.echr.coe.int/webservices/content/ pdf/001-76586,).

[239] *See* PPD-28, *supra* note 96.

[240] *See id.*

shared, a definition of the purposes for which states may exchange intelligence information provides greater utility in parsing foreseeable exchanges.

Category [3] and [6] highlight the procedures governing temporal limitations on information sharing. While the sharing of analyzed information does not contain a temporal aspect, joint intelligence ventures collecting raw information could persist for an undisclosed amount of time. As a result, intelligence-sharing laws should incorporate procedures for determining the appropriate duration of raw intelligence sharing operations. All transferred information could be subject to a sunset clause requiring the erasure of shared intelligence information after six months absent explicit reauthorization.[241]

Category [4] concerns important procedures related to accessing, retaining, and storing transferred information. The procedures should address technological procedures related to the safe storage of intelligence information in a secure server, record keeping procedures, and logs to account for the use or forensic inspection of the information use. Moreover, while analyzed information should be appropriately tailored to the scope of the request, both raw intelligence and analyzed intelligence will usually contain personal information, and the transfer of such information should not result in a total abdication of access controls. Therefore, states should clarify the scope of their access controls and related procedures. For example, the German surveillance authorization act examined in *Weber* provided "detailed rules on storing and destroying any data obtained using these search terms, and the authorities storing the data had to verify every six months whether the data were still necessary to achieve the purpose for which they had been obtained or transmitted to them."[242]

Access controls are especially important given the variation in the conceptualization of privacy harms. On the one hand, European Courts have found that "that the storage of private information amounts to or is akin to

---

[241] *See, e.g.*, Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses [Artikel 10-Gesetz] [G 10] [Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications] [Article 10 Act], June 26, 2001, BGBl. I at 1254, 2298, as amended, http://www.gesetze-im-internet.de/bundesrecht/g10_2001/gesamt.pdf (requiring authorities storing the data had to verify every six months whether the data were still necessary to achieve the purpose for which it had been gathered).

[242] Rubinstein et al., *supra* note 30, at 113.

secret surveillance."[243] Under this conception, the mere collection of information constitutes a privacy harm. However, many states take a different approach to data access and argue that "[u]ntil the data are accessed by humans and used as a means of investigating or identifying particular people . . . , no concrete intrusion has occurred."[244] As Deeks reports, "states seem committed to the idea that they require access to as much data as possible to accurately locate terrorist plots and connections among suspected terrorists, among other threats."[245] Both offer legitimate approaches to balancing

---

[243] Matthew White, *Protection by Judicial Oversight, or an Oversight in Protection?*, 2 J. INFO. RTS., POL'Y, & PRACTICE 1, 33 ("The ECtHR has previously noted that e-mail and internet usage fall within the ambit of Article 8334 and on numerous occasions has held that the storage of private information amounts to or is akin to secret surveillance."). *See also* Lubin, *supra* note 51, at 515 ("As was explained by Commissioner Pillay, an interference with the right to privacy already occurs at the point of interception.").

[244] Christopher Slobogin, *Policing, Databases and Surveillance: Five Regulatory Categories*, 28 (Nat'l Const. Ctr. White Paper Series, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551164 ("It is further assumed by the intelligence community that the infringement of the data subjects' rights takes place only at the point at which their data is retrieved from the "haystack on the basis of a search term, keyword, or other selector."). Deeks points to some United States courts that have taken this approach. Deeks, *supra* note 51, at 357 ("This is consistent, for instance, with the approach some U.S. courts have taken to the Fourth Amendment; for them, a search (and therefore an infringement on privacy) occurs when information is exposed to possible human observation, rather than when it is copied or processed by a computer."). *But see* Daskal, *supra* note 62, at 354 (cataloging the "rich and thick literature" contending that simple data collection inflicts severe privacy harm); Neil M. Richards, *The Dangers of Surveillance*, HARV. L. REV. 1934, 1936 (2013), https://ssrn.com/abstract=2239412 (arguing that surveillance "menaces intellectual privacy and increases the risk of blackmail, coercion, and discrimination" and should comprise a harm sufficient for constitutional standing).

[245] Deeks, *supra* note 51, at 357. Such logic proceeds as follows: The retention of information is critical because one cannot know when it will come in handy. One can analogize to the use of Box, Dropbox or an external hard drive. You never know which document is going to crash, so you back up all documents. Similarly, with intelligence collection—there is a vast degree of available information, and intelligence officials don't know what will come in handy later down the line. While one might push back to suggest that, using the back-up example, there is no need to save every piece of information. Instead, one prioritizes different documents to different degrees. For example, losing a shopping list would carry far less severe consequences than the loss of a 70-page research paper. However, such an argument misunderstands the nature

privacy and security.[246] Brown et al disagree, arguing that the latter approach "cannot be reconciled with international human rights law."[247] However, Brown and his colleagues ground their claim of international human rights law on *European* human rights law; thereby conflating the privacy-security tradeoff for one regime with that of the entire international community.[248]

Nevertheless, the differing points of restriction should encourage states to consider access control safeguards. States that impose a higher barrier to data

---

of data retention. The problem with discordant pieces of information is that, prior to an incident in question, one does not know which information will prove most necessary. As such, the more appropriate analogy would be to ask which sources would prove most valuable at the very onset of a research project. Without knowing the direction of the project, it can be nearly impossible to know which information to prioritize in advance.

[246] The collection process and storage of information, in addition to the distribution of information under the control of private companies versus government entities are important questions beyond the scope of this discussion.

[247] Brown et al., *supra* note 199.

[248] To be sure, Brown et al. is correct as a matter of European law. The Court in Szabó & Vissy v. Hungary, App. No. 37138/14, Eur. Ct. H.R., Judgment, ¶ 78 (2016), http://hudoc.echr.coe.int/eng?i=001-160020, recognized that mass surveillance could undermine citizen freedom if all privacy barriers were eliminated.

Indeed, it would defy the purpose of government efforts to keep terrorism at bay, if the terrorist threat was paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives.

However, such a portrayal rests on the notion that there must in fact be an intrusion—that information is actually accessed. It is also true that the Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, argued that despite "[t]he prevention and suppression of terrorism [being] a public interest imperative of the highest importance," bulk collection programs "pose a direct and ongoing challenge to an established norm of international law." Ben Emmerson (Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism), *Promotion and protection of human rights and fundamental freedoms while countering terrorism*, U.N. Doc. A/69/397 (Sep. 23, 2014). However, United Nations officials' pontifications on international law do not determine the state of international law.

collection tend to employ fewer safeguards at the data access phase.[249] In contrast, states that do not consider privacy interests at the collection state will likely employ measures that restrict access to more limited criteria of conditions and circumstances.[250] Thus, access procedures for transferred data should include measures to condition access to exchanged information, even if state surveillance practices do not contain any access requirements.[251] Conditioning access on state-specific safeguards—further expanded in Part 0—plays a critical role in protecting the legitimate privacy interests in disparate privacy-security regimes.

Finally, Category [5] concerns third party transfers. As such, it necessarily incorporates all of the suggested procedures and principles outlined in this framework for cross-border intelligence sharing. However, it also concerns onward transfers from the receiving agency. The onward transfers may be internal; many countries have seen a decline in the "wall" separating national security and other law enforcement uses.[252] Intelligence transfers should be limited to national security purposes, and measures should be undertaken to maintain a wall over transferred information. If the recipient country would also like to access shared intelligence for law enforcement purposes, it should pursue that information through the appropriate channels. Intelligence sharing should not serve as a shortcut around MLAT agreements.

---

[249] For example, the United Kingdom, which imposes collection restrictions, does not distinguish between collection and access. DAVID ANDERSON, A QUESTION OF TRUST–REPORT OF THE INVESTIGATORY POWERS REVIEW, 292-94, 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf (illustrating that the United Kingdom does not distinguish between collection and access).

[250] *See* Rangappa, *supra* note 36 (discussing the United States bulk data collection pursuant to § 702 which contain access protections that ensure that "neither the metadata nor the content of that communication is immediately accessible to all agents.").

[251] *See* Deeks *supra* note 51, at 305 (explaining the United States permits surveillance as long as its surveillance is consistent with transparent laws and furthers a legitimate aim but does not require proportionality or necessity).

[252] Rubinstein et al., *supra* note 30, at 105 ("In many countries, this wall has been dismantled, with the result that intelligence agencies may now, at least as a matter of legal authority, pass information to law enforcement officials. . . .").

The receiving agency might also seek onward transfers of shared information to external parties. Governments receiving information should commit to ensuring that exchanged intelligence information is not shared with non-governmental parties. However, government intelligence agencies should have the flexibility to share such information with other government intelligence partners, in the event that the receiving party commits to the same transfer restrictions as binding the original recipient. Of course, governments have no obligation to share information with a third party, and political considerations effectively restrain third-party intelligence sharing against the originator's wishes. Integrating data access and data sharing procedures would help offset a major barrier to intelligence sharing: the difficulties that countries face in verifying how a foreign government will use information sent to it.[253]

In sum, safeguards against abuse should include 1) public limitations on the purposes of government intelligence sharing; 2) public limitations on the duration of sharing agreements and the implementation of sunset clauses; 3) public access, retention, and storage procedures for exchanged information; 4) and public commitment to third-party transfer procedures ensuring that exchanged intelligence information remains limited to government intelligence use.

iii. Principle of Transparency and Oversight

Intelligence sharing agreements should not operate in a vacuum of accountability. The UN General Assembly Resolution on the Right to Privacy in the Digital Age, which calls upon all states "[t]o establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data . . ."[254] Furthermore, modern norms have led to a public

---

[253] BORN ET AL., *supra* note 4, at 38 ("[I]ntelligence services lose full control of information as soon as they transmit it to another body.").

[254] G.A. Res 69/166, at 4 (Dec. 18, 2014). *See* Emmerson, *supra* note 248 ("One of the core protections afforded by article 17 is that covert surveillance systems must be

expectancy of greater transparency over intelligence activities.[255] By establishing publically available governance measures for intelligence sharing agreements, states will take significant steps towards transparent practices. While the government cannot provide complete transparency to the public, it can provide more searching internal oversight procedures.

Intelligence sharing agreements would benefit from the designation of a specific independent official or officials responsible for overseeing intelligence sharing exchanges and subsequent access. Many countries already have independent oversight of surveillance and government access, with China as a notable exception.[256] Significantly, independent oversight does not implicate the government's chosen privacy-security tradeoff, but instead ensures that intelligence information is handled commensurate with that government's standards. For example, the United States has a Privacy and Civil Liberties Official who ensures the legitimate privacy interests of data handled by the intelligence community.[257] Such a role should operate similarly to Inspector Generals, embedded in United States executive agencies.

In order to effectively implement intelligence transfer access controls, each country must implement *ex ante* review. This oversight process already exists through Sweden's Defense Intelligence Inspection (SIUN) body, which monitors whether the procedural conditions have been complied with before transferring the information in question for use by Swedish intelligence.[258]

---

attended by adequate procedural safeguards to protect against abuse. These safeguards may take a variety of forms, but generally include independent prior authorization and/or subsequent independent review."). However, the Special Rapporteur goes too far in asserting the mass collection schemes are necessarily inconsistent with principles of individualized suspicion.

[255] Deeks, *supra* note 63, at 618 ("Overall, the public now expects greater transparency about intelligence activities and some governments have begun to provide it.").

[256] Rubinstein et al., *supra* note 30, at 104.

[257] PPD-28, *supra* note 96 (describing the principles of United States signals intelligence collection).

[258] European Commission for Democracy through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, CDL-AD(2015)006, Study No. 719/2013, ¶¶131-133 (Apr. 7, 2015), http://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-AD(2015)006-e ("An example of a model which combines judicial authorization with expert follow-up comes from Sweden.").

Former Independent Reviewer of Terrorism Legislation David Anderson has proposed a series of possible *ex ante* criteria that the UK could implement for bulk data access.[259] This *ex ante* review requirement aligns with a CJEU emphasis on the importance of independent authorization.[260] When assessing government access to retained data, the CJEU has held that all access should "be subject to a prior review carried out either by a court or by an independent administrative body."[261] Prior review constitutes a best practice and should be implemented across all states. Oversight independence should be established through the criteria that 1) the overseer can only be removed for cause; 2) the overseer is not appointed by the executive branch; and 3) the overseer is not involved in the intelligence exchange mission.

Professor Richard Aldrich conceives the possibility of "Inspectors General with extended authority to operate in more than one country."[262] Given that countries will display a variety of different procedures and processes, a roving Inspector General should not be a requirement for sharing compliance. Nevertheless, a joint Inspector General would add particular value in joint raw data collection enterprises. These joint enterprises, such as the compilation of joint databases, poses greater privacy risks and would be well-served by another layer of protection. Furthermore, this close-knit form of "far reaching" cooperation is only likely to occur if the states maintain a "close,

---

[259] ANDERSON, *supra* note 249, at 292–94 (following the British model which does not distinguish between collection and access).

[260] *Ex ante* authorization is not a uniquely European requirement, and the U.S. has played a significant role in promulgating an *ex ante* review ethos. As Jennifer Daskal reports, "[t]he UK government supported a new judicial review mechanism for intercept orders in part because it knew that this would be a precondition entering into such an agreement under US law." Jennifer Daskal, *New Bill Would Moot Microsoft Ireland Case—And Much More!*, JUST SEC. (Feb. 6, 2018), https://www.justsecurity.org/51886/bill-moot-microsoft-ireland-case-more.

[261] Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-Och telestyrelsen, 2016 EUR-Lex 62015CJ0203 (Dec. 21 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN ("In order to ensure, in practice, that those conditions are fully respected, it is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body[.])".

[262] Aldrich, *supra* note 9, at 56.

trust-based relationship."[263] Given the muted secrecy concerns, such a cooperative arrangement with an objective third-party Inspector General is conceivable for a subset of states with a high commitment to public transparency.[264] Such bodies could operate along lines similar to the International Committee for the Red Cross (ICRC) in its designation and ability to inspect treatment of prisoners of war,[265] or the International Atomic Energy Agency (IAEA) mandate to inspect nuclear sites. Specifically, joint intelligence operations could include an arrangement to allow an objective party to inspect and provide reports on compliance of procedural privacy safeguards.[266]

Intelligence sharing agreements should also require states to include a measure of *ex post* review to ensure that the surveillance measures undertaken are done so according to the procedures in place. Particularly when security exigencies require urgent government action, *ex post* review provides prospective control over future behavior. As the ECtHR recognizes "a subsequent judicial review can offer sufficient protection if a review procedure at an earlier stage would jeopardise [sic] the purpose of an investigation or

---

[263] BORN ET AL., *supra* note 4, at 19.

[264] *See* Aldrich, *supra* note 9 (suggesting inspectors general with extended authority in more than one state).

[265] *See, e.g., Rule 124. ICRC Access to Persons Deprived of Their Liberty*, INT'L COMM. RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule124 ("The right of the ICRC to visit detainees in international armed conflicts is provided for in the Third and Fourth Geneva Conventions.").

[266] Preexisting bilateral and multilateral exchanges between external oversight bodies might provide a foundational framework for building international acceptance. Examples of such bodies include "periodic meetings with national parliamentary oversight committees organized by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs; the annual Southeast European Parliamentary Oversight Bodies' Conference; the biennial International Intelligence Review Agency Conference (IIRAC); and the (now defunct) Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States." BORN ET AL., *supra* note 4, at 156. An institutional entity could also provide other benefits, such as a rigorous training program that could provide best practices for privacy protection. Such a training program could help promote responsible handling of personal information and diminish the fears of privacy harm stemming from intelligence practices. *See* Kent, *supra* note 186, at 12 (recommending international standards of training for law enforcement data requests).

surveillance."[267] Domestic audits offer one effective form of *ex post* review. Such an inspection process should occur at regular intervals, with reviewable information based on the time of access or, in exceptional circumstances, as promptly as possible. In addition, an oversight body could scrutinize the procedural compliance through methods such as hearings, documentary analysis, interviews and sampling.[268] Scheduled inspections could be further supplemented by surprise visits. In Norway, a national model is already in place, where the Parliament's Intelligence Oversight Committee (EOS) has the power to conduct surprise inspection visits for shared data.[269]

Finally, each state should provide whistleblower protection in the event of abuse of intelligence sharing agreements. Given the sensitivity of intelligence operations, whistleblower protections do not need to extend to the release of information to the public.[270] However, each state should ensure that government employees or officials may report violations of protocols and procedures to the relevant oversight bodies without fear of retribution.

iv. Principle of Proportionality

States disagree about the need for a proportionality analysis in their own surveillance operations. The United States, for example, only requires surveillance to meet a legitimate national security purpose, but the European Union requires proportionality.[271] The ECtHR in *Weber and Saravia* established

---

[267] Sommer v. Germany, App. No. 73607/13, Eur. Ct. H.R., 15 (2016), http://hudoc.echr.coe.int/eng?i=001-173091. However, this model contests the ECtHR's' subsequent proclamation that "the effectiveness of a subsequent judicial review is inextricably linked to the question of subsequent notification about the surveillance measures. There is, in principle, little scope for recourse to the courts by an individual unless he or she is advised of the measures taken without his or her knowledge and thus able to challenge the legality of such measures retrospectively." *Id.*

[268] BORN ET AL., *supra* note 4, at 147-48 (discussing some principle methods of review for data sharing).

[269] *Id.* at 148.

[270] This more circumscribed view almost certainly departs from the whistleblower protection envisioned by the Snowden Treaty Advocates calling for "international protections for whistleblowers." *The Snowden Treaty*, *supra* note 195.

[271] *See* Deeks, *supra* note 51 (assessing the differences between the United States' and the ECtHR approach).

a European balancing test that weighs "all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law."[272] Countries will continue to differ in their decisions whether to insert proportionality considerations in their intelligence practices. Nonetheless, when it comes to sharing intelligence, proportionality considerations should not be wholly absent from either the sharing or accessing of foreign intelligence information.

First, states should condition their access of shared intelligence information on a proportionality assessment. In order to access foreign analyzed intelligence information, states should engage in a balancing analysis weighing the degree of privacy intrusion, demonstrated by the nature of the data sought and the amount of data sought,[273] against the specific purpose for which the information is being accessed. It is important to note that the privacy intrusion calculation should focus on the *content and volume* of the information shared, and not the means by which that content was collected. While some might prefer that all foreign intelligence include the means by which such intelligence was collected, foreign states will not realistically divulge such information in most circumstances. Moreover, attempting to apply procedural collection processes across countries fails to account for the fact that another agency could have gathered the same information through a different process. For example, one intelligence agency might have obtained telephone records through a targeted bulk data collection, and another agency might have obtained the same telephone records with a warrant—or would have been able to do so if the relevant telephone company were located under its jurisdiction.

Nevertheless, states' domestic legislatures should retain significant leeway in applying access controls for accessing foreign-sourced analyzed information. These legislatures could prescribe the weight given to different factors in a proportionality assessment. For example, the United States might

---

[272] Weber & Saravia v. Germany, App No 54934/00, 2006-XI [2006] Eur. Ct. H.R. 1173, Admissibility, 24 (2006), http://hudoc.echr.coe.int/webservices/content/pdf/001-76586.

[273] Slobogin, *supra* note 244.

decide that U.S. intelligence services might only access foreign intelligence reports that target non-U.S. citizens. Alternatively, the U.S. might require the anonymization of U.S. citizen's personal information unless granted permission to reinsert redacted information by the FISA court. Any such access controls should be implemented by the receiving state. Through such a process, domestic legislation could control the parameters and risk of incidental use of domestically unattainable information. As explained in Part 0, this process should be further bolstered by internal oversight to ensure that intelligence agencies do not abuse foreign intelligence sharing to circumvent their own collection limitations. Due to widely differing privacy-security tradeoffs, the access standards would likely exhibit wide variation. This framework does not recommend substantive access standards beyond the exigency exception in Part 0, but instead urges substantial flexibility in allowing sovereign states to determine the content of its access controls.

States could create more robust access barriers that include collection methods for the transfer of raw intelligence. Since raw intelligence has not been altered from its initial collection form, its mode of collection is far more easily discernable. If sharing raw intelligence, states should be willing to either disclose the intelligence collection method or stipulate that the collection method would not have violated the intelligence collection laws of the partner state. Joint overseers, as suggested by Aldrich,[274] could facilitate the more rigorous implementation of state-specific access controls.

States should also avoid transferring requested information without the partner state sharing a purpose or justification. Due to access control variations in state intelligence practice, states should adopt a limited proportionality assessment requiring legitimate justification when they consider intelligence requests by foreign intelligence partners. Specifically, states should confirm that their partners would use the information for a legitimate purpose. The implementation of the proportionality requirement might not substantively differ from the requirement to meet a national security purpose. However, the articulation of justification and oversight review will ensure that the shared intelligence information is only used in a

[274] *See* Aldrich, *supra* note 9.

manner consistent with that state's privacy security balance. Such analyses should apply to requests for both metadata and "content" data.[275]

Before transferring information to foreign intelligence partners, government intelligence officials should explicitly account for privacy interests in addition to security and political calculations. Nevertheless, the international community would be ill-served by the adoption of a "necessity" principle for data sharing. The UN Human Rights Experts' Brief in *Kidane* provides an operational definition for necessity:

> The requirement of necessity implies that restrictions must not simply be useful, reasonable or desirable to achieve a legitimate government objective. Instead, a State must demonstrate "in specific and individualized fashion the precise nature of the threat" that it seeks to address, and a "direct and immediate connection between the expression and the threat.[276]

Such a necessity requirement would force intelligence agencies to disclose national security threats to their partners and would also require admission of domestic vulnerabilities and weaknesses in their own national security regimes. Additionally, states differ in their perceptions of necessity based on potentially private information about the nature of domestic risks. Governments would likely be unwilling to disclose such information.[277] As

---

[275] Courts have increasingly recognized that both content data and metadata invoke significant privacy concerns. *See, e.g.*, Joined Cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-Och telestyrelsen, 2016 EUR-Lex 62015CJ0203, ¶ 199 (Dec. 21 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62015CJ0203&from=EN ("data [that] provides the means . . . of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications."); United States v. Jones, 565 U.S. 400, 416 (2012) ("And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

[276] Brief of Amici Curiae United Nations Human Rights Experts in Support of Plaintiff-Appellant and Reversal at 14, Doe (Kidane) v. Fed. Rep. of Eth., 851 F.3d 7 (D.C. Cir. 2016) (No. 16-7081), 2016 WL 6476760.

[277] *See* Arar v. Ashcroft, 585 F.3d 559, 576 (2009) ("Even the probing of these [exchanges among the ministries and agencies of foreign countries on diplomatic, security, and intelligence issues] entails the risk that other countries will become less willing to cooperate with the United States in sharing intelligence resources to counter terrorism.").

such, the state requesting the information is best situated to evaluate its need of the information. While state with the information may refuse an intelligence request for any number of reasons, requiring a state to conduct a necessity test before transferring intelligence information would not serve the public world order in facilitating critical intelligence transfers.[278]

v. Principle of Notification and Remedies

International human rights law also contains the principle of notification and remedies. Many states do not provide notifications of data use, and remedies vary widely across states. For intelligence sharing purposes, states should require notification to the originator state when the recipient state substantively accesses private information. Such provisions should also include flexibility for the state to delay notification for a limited period of time pursuant to ongoing operations. Mandatory state notifications would reduce information barriers and facilitate cooperative international self-governance. Moreover, any private right of action should be conditioned upon the principle of sovereign consent.

Procedures for individual notification should rest on the specific state laws, and the state should have discretion over the circumstances and timing of notification that personal information has been accessed. The originator state should also control the degree of disclosure, or the level of specificity of which information was accessed or by whom. Importantly, the notification procedures should be codified into law. This process will create political accountability, and the scope of government notification commitments should respond to the political process.[279]

A state-based notification system places the state as a guardian *ad litem*, charged with protecting the best interests of its citizens. In practice, intelligence sharing is policed by the understanding that violations "will be

---

[278] *See, e.g.*, UK IPT Response, *supra* note 219, at ¶208 (contending that "power to share intelligence with a foreign intelligence agency must plainly be capable of being 'necessary'").

[279] Admittedly, autocratic governments will tend to be less responsive to political pressure. However, the process of requiring even those governments to publically adopt a stance; even a zero-notification policy generates political pressure and encourages accountability.

sanctioned by reduction or cessation of future cooperation."[280] As such, if intelligence officials have reason to believe their intelligence partners are misusing shared information, they should think twice before participating in future intelligence exchanges. While intelligence officials may have incentives to turn a blind eye to privacy intrusive practices, the presence of independent oversight bodies will lead to official compliance with domestic laws regarding sharing notification procedures.

Additionally, sovereign immunity principles weigh against allowing a private right of action absent state consent. Generally, sovereign governments are immune from lawsuits except to the extent that a government consents to a waiver of its immunity.[281] Sovereign immunity has also crystalized into a principle of customary international law forbidding suits against sovereign states in foreign jurisdictions without the states' consent.[282] Taken together, principles of state and international respect for sovereign immunity weigh against forcing a sovereign immunity waiver for an individual right of action. Nevertheless, the absence of a private right of action does not mean that individual privacy interests should remain untended. As explained above, the state has a responsibility to protect the privacy interests of its citizens. Against this backdrop, the cooperative nature of intelligence sharing leaves room for pressure and leverage through informal processes to deter future privacy violations. Finally, state oversight bodies have jurisdiction over privacy violations, and depending on the individual notification procedures, states can establish processes by which individuals or state representatives may bring claims against the government for procedural or substantive harms incurred as a result of an intelligence-sharing agreement.[283]

---

[280] BORN ET AL., *supra* note 4, at 38.

[281] *See, e.g.*, United States v. Sherwood, 312 U.S. 584, 586 (1941) ("The United States, as sovereign, is immune from suit save as it consents to be sued.").

[282] Xiaodong Yang, *Sovereign Immunity*, OXFORD BIBLIOGRAPHIES, (May 25, 2016), http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0018.xml.

[283] Ian Brown has gone so far as to suggest that "illegal surveillance should be criminalized." Brown, *supra* note 154, at 31. While states have the flexibility to criminalize surveillance activities, considerations underlying the United States' discretionary function exemption of official immunity likely applies here—namely, in

vi. Principle of Complementarity

Another important international law principle relevant for intelligence sharing concerns complementarity. The principle of complementarity "counsels deference based on both the imperatives of sovereignty and other provisions of international law, including the law of armed conflict and U.N. Security Council resolutions that require global cooperation to combat terrorism."[284] In the realm of privacy rights, complementarity encourages allowing a margin of flexibility for how states apply those rights in practice vis-à-vis security interests. The European Court of Human Rights recognized such a complementarity principle in *Leander v. Sweden*, holding that Sweden had a wide "margin of appreciation" when choosing the means for achieving the legitimate aim of protecting national security.[285]

When applied to intelligence sharing, the traditional complementarity principle receives reinforcement by the notion of international comity, or the idea that states should adjudicate their laws in a way that "respect[s] the sovereign rights of other nations by limiting the reach of its own laws and their enforcement."[286] Concerns of comity should provide states with special flexibility in arranging intelligence sharing agreements. Specifically, this principle encourages states to grant greater deference to state national security practices than they might otherwise exercise in other contexts. The principle of complementarity provides the flexibility necessary to facilitate intelligence sharing in a world of differing privacy-security tradeoffs.

vii. Principle of Good Faith

The principle of good faith must govern intelligence sharing arrangements. Namely, all information requests and request fulfillments should be carried out in good faith. Such an obligation mimics the good-faith exception to the

---

protecting the officials from "liability that would seriously handicap efficient government operations." United States v. S.A. Empresa de Viacao Aerea Rio Grandense *(Varig Airlines)*, 467 U.S. 797, 814 (1984).

[284] Margulies, *supra* note 173, at 2139.

[285] Leander v. Sweden, App No 9248/81, 9 Eur. H.R. Rep. 433 at ¶59 (1987).

[286] Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108, 128 (2013). *See generally* Jesner v. Arab Bank, 138 S. Ct. 1386 (2018) (tackling questions of international comity).

United States' Fourth Amendment exclusionary rule. United States courts generally do not permit the use of evidence collected in violation of the Fourth Amendment.[287] However, this exclusionary rule does not apply when an official conducts a search or seizure with a reasonable good faith belief that the search was consistent with the rule of law.[288] Similarly, national intelligence agencies should be able to share and utilize shared information as long as they have a reasonable good faith belief that both they and their intelligence partners have complied with the agreed-upon legal procedures.[289]

This good faith principle plays a critical role in respecting the obligation that states do not use intelligence-sharing practices to circumvent domestic safeguards through revolving door tactics. United States Executive Order 12333 establishes such a principle for U.S. conduct, and forbids members of the United States intelligence community from participating in or requesting any activities that they could not lawfully carry out themselves—including intelligence collection.[290] Similarly, good faith privacy protection motivates the tailoring of information delivered in the course of surveillance requests. To the extent that domestic regimes of a receiving state provide higher standards of protection on a given issue, such as limitations on the use of national's information, the presence of an independent oversight apparatus can also facilitate good-faith compliance.

Just as states should not request foreign intelligence agencies to engage in unlawful practices, states should also not share data that they know the partner states could not collect. Instead, foreign states should undertake a good-faith effort to avoid sharing information that, to a non-trivial degree, relies on information that their intelligence partner could not have lawfully collected. This should not impose an obligation on states to comb their

---

[287] Mapp v. Ohio, 367 U.S. 643, 657 (1961).

[288] United States v. Leon, 468 U.S. 897, 909 (1984) ("[T]he exclusionary rule be more generally modified to permit the introduction of evidence obtained in the reasonable good-faith belief that a search or seizure was in accord with the Fourth Amendment.").

[289] Of course, the good faith "use" of information here differs from the exclusionary rule context; while the exclusionary rule is concerned with evidentiary inclusion, intelligence sharing involves utilization by information by other intelligence operatives.

[290] Exec. Order No. 12,333, 3 C.F.R. 200, § 2.12 (1982).

analyzed intelligence reports to prevent any incidental disclosure of private information. Rather, the sharing states should make a good-faith effort to provide the information that the receiving state needs for implementing its access controls. For example, the United States might request a threat assessment of a particular organization from Great Britain, and that report might contain some information through a method that the receiving state could not have undertaken. The United States might not allow for foreign intelligence containing personal information on U.S. nationals in the absence of a warrant. In order for U.S. intelligence agencies to access the report, they might need to meet legislated access controls that require an independent authorizer to attest that the report does not contain information about U.S. citizens. If so, then the U.S. intelligence sharing request could request that the U.K. specify whether the report contains information about U.S. citizens so that the U.S. agency can undertake the necessary steps for authorized access. The UK should make a good faith effort to comply with such a request. If states adopt limitations that are too exacting, these exclusions could impose significant costs on each party. Including stakeholders from the intelligence agencies when designing access controls will go a long way towards minimizing the costs of such information requests.

Without good faith, state intelligence sharing cannot operate out of the public eye. The intelligence sharing system must therefore be established in a fashion that breeds public trust in the processes and procedures undergirding these covert operations shrouded in secrecy.[291] As former U.S. President Obama commented in light of United States anti-terrorism tactics, "If people can't trust not only the executive branch but also don't trust Congress and don't trust federal judges to make sure that we're abiding by the Constitution, due process and rule of law, then we're going to have some problems here."[292] Public faith in the good will of the intelligence community is foundational to a robust security establishment. However, state security interests do not require blind faith. Good faith principles combined with publically available procedural safeguards can help shore up popular legitimacy. Taken together,

[291] For a list of benefits that arise from maintaining the secrecy of intelligence cooperation, see Deeks, *supra* note 224.

[292] *See* Nicholas & Gorman, *supra* note 34.

these seven principles allow for public disclosure and facilitate accountability without undermining the privacy-security tradeoff.

viii. Exigency Exception for Non-Compliant States

This framework should also anticipate that not every state would immediately adopt these principles. For the reasons outlined above, an effort to completely block intelligence sharing with non-compliant states would be both impractical and highly dangerous for all states involved. So how should states approach states who lack the important safeguards outlined in this framework? First, it is clear that intelligence agencies should be limited in their ability to share information with countries that do not adopt the policies consistent with the principles above. Nonetheless, not all intelligence sharing directly implicates individual privacy rights. As such, states can still share and receive strategic and operational information with non-compliant intelligence partners as long as the information does not contain personally identifiable information. For example, important policy analyses related to foreign policy developments or general threat assessments of a particular group will not necessarily disclose personal information.[293]

One might imagine a situation in which an intelligence agency discovers information necessary to prevent a serious threat to the welfare of another state. In such circumstances, an exigency exception should prove appropriate. Specifically, this exigency exception should allow agencies to provide or receive necessary information, even if it includes personal information, in the limited scenario of a high-probability event that reasonably threatens the loss of life or substantial disruption to core operational services. Furthermore, the state must reasonably believe that the additional information presents "material" information germane to the reduction of the threat. Under these limited circumstances, non-compliant foreign partners may share intelligence information under the exigency exception. However, due to information asymmetries, the receiving state may realize that the shared information does not actually meet the exacting exigency standards. In these situations, the

[293] While one can make the case for a public figure exception whereby public figures enjoy diminished privacy protections, such an exploration lies beyond the scope of this Article.

receiving state should still be able to utilize the information as long as it determines that the information was shared in good faith.

The presence of exigent circumstances does not relieve a state of its responsibility to protect individual privacy. When states share information under such circumstances, they should seek to tailor the information granted to the specific request. When transferring information, states should limit sharing personally identifiable information to the extent reasonable. As part of this effort, states should avoid sharing raw intelligence data whenever feasible, and should instead convey the necessary information through analyzed "end product" intelligence. Additionally, compliant states should request that states receiving such intelligence only use this information for its intended purpose, although such an endeavor is unlikely to have any practical impact.

While this framework sets the expected standards to govern state transfers of intelligence information to non-compliant states, states may carve out additional exceptions. While recipient states would not have the ability to share intelligence information received from framework-compliant states, all states would still retain the sovereign discretion to engage in additional sharing agreements with other states. However, any information received from non-compliant states would still be subject to the procedural requirements detailed above. While deviations from this framework would likely be domestically unpopular, one could imagine popular limited exceptions, such as one that allows countries to share information related to border migration, regardless of internal governance standards.

This exigency exception should also apply to intelligence sharing among framework-compliant states. Specifically, the framework should allow the transfer of "exigent" information that would otherwise be barred due to revolving door concerns. Finally, in accordance with the principle of legality, states should undertake to codify the parameters of this exigency exception into domestic law.

D. Application

This Section seeks to concretize the above framework by testing the suggested framework against plausible scenarios. The scenarios focus on bilateral

intelligence sharing. Each of the below scenarios explore the actions that State A must take to comply with the proposed intelligence-sharing framework.

i. Scenario One: Sharing Intelligence

Suppose that State A's intelligence agency, while conducting surveillance in accordance with its domestic laws, intercepts six text message communications between two foreign nationals. The intercepted messages displays sympathies with a designated terrorist group's political goals, and mentions a willingness to further the group's cause in their home countries, States B and C. State A's intelligence agency would like to share this information with States B and C. However, State A has adopted laws implementing the proposed framework through public statutes, as required by the legality principle. How does State A proceed?

State A must initially assess whether it can share the gathered information with States B and C. This assessment raises two questions. First, States A's intelligence community will need to look to the procedural requirements that State A has legislated into domestic law to determine whether sharing this information serves a legitimate purpose. State A will have legislated public limitations on the purposes of government intelligence sharing in according with the Principle of Safeguards Against Abuse. Let us assume that the legitimate purposes include the sharing of information to prevent threats to terrorism and national security, serious crimes, and threats to public safety. As such, the proposed information sharing would meet legitimate goals under the statute.

Next, State A must assess whether States B and C have adopted this intelligence-sharing framework. Let us assume that State B has adopted the framework, but State C has not. This difference leads the analysis to diverge for the subsequent steps of the intelligence sharing process. Let us first focus on State B.

Because State B has adopted procedures consistent with the intelligence sharing framework, State A can easily assess State B's public laws to confirm that its intelligence sharing procedures provide the necessary procedural protections. Specifically, State A can confirm that State B has safe information storage procedures, has temporal limitations on the retention of shared

information, and will not engage in third- party transfers, except with intelligence agencies who have adopted this same framework.

Under the sharing framework, State B will also need to conduct a proportionality test before accessing such information, balancing the nature of the data sought and the amount of data sought against the specific purpose for which the information is being accessed. Due to the fact that State B did not request the information (and therefore does not know enough to conduct the analysis), State A will need to explain the general nature of the intelligence. In this case, State A's explanation would detail the fact that State A identified text messages suggestive of a high-risk individual interested in aiding the terrorist's goals. State A would then deliver those six messages. An independent oversight officer in State B would then need to conduct a proportionality test before accessing that information. In this case, the government purpose would be to identify high-risk individuals for national security and the privacy intrusion would comprise the six messages, as well as the cell phone numbers of the communicators. Oversight officers in State B would liaise with officers in State A to ensure that State B has enough information to apply its domestic access controls.

State B, after having accessed this information and finding cause for serious concern, might believe that more of the text messages contain important information. State B might request State A to transfer all intercepted text messages by one of the communicators for a three-month time frame. However, State B can only request such information if State B believes in good faith that State B's domestic law would allow the intelligence agency to lawfully intercept these messages. Even if State B would be legally permitted to obtain such information, the Principle of Safeguards Against Abuse requires State B to condition any access to the transferred text messages in line with all legislated access controls.

The intelligence agencies in State A and State B would have the advice and counsel of their respective oversight officers as they transferred, processed, and accessed the shared information. Moreover, each agency would be subject to governmental audits to facilitate an *ex post* review. Once State B accesses the transferred intelligence data, State B must inform State A. State A will then

follow its domestic laws governing the relevant notification procedures to the parties in question.

State A must take a different approach with State C. State C has not adopted the intelligence-sharing framework. As such, State A faces more limited options. State A can only share information if it falls into the exigency exception—namely, a high-probability event that reasonably threatens the loss of life or substantial disruption to core operational services. The identification of potentially dangerous terrorist sympathizers would not meet this high standard. Therefore, State A would not be able to share this intelligence information with State C (unless States A and C have negotiated a separate bilateral agreement). However, State A's inability to share the text messages does not mean that State A is completely hamstrung. State A can still warn State C without divulging any personal information. For example, State A might inform State C that they have reason to believe that State C has terrorist sympathizers in their country, and State C should exercise vigilance. In the event that State A later learned that one of the identified sympathizers has purchased explosives in preparation for a terrorist plot, State A would be able to share information with State C under the exigency exception. However, State A should avoid sharing raw intelligence information, and instead provide a report to State C identifying the suspect and the nature of the threat.

ii. Scenario Two: Receiving Intelligence

Imagine that through the course of its lawful intelligence practice, State A's intelligence services discover that two foreign individuals, residing in State B and citizens in State C, are likely involved in a plot against State A. State A only has limited intelligence on these individuals. As such, State A contacts its intelligence partners in State B and C to learn if they can provide information related to these two individuals and assist in their threat assessment. State B has adopted the proposed intelligence-sharing framework; State C has not.

State B has also observed these two State C nationals with concern, and through an extensive bulk collection program, has pulled the raw communications data for these two suspected individuals for the last three

months, and has compiled analyzed reports. State B finds that State A's request meets a permissible purpose and has established procedures in accordance with the intelligence-sharing framework. After ensuring that the shared information is reasonably tailored to State A's request, State B shares its analyzed reports and communications interceptions with State A.

State A cannot access the communications information without applying its own access controls. Imagine that State A's legislature has enacted rules that forbid its intelligence community to use bulk interception practices to gather information on any person and does not allow the access of foreign intelligence concerning any State A nationals without a judicial warrant. Before accessing the transferred information, an independent authorizer in State A would need to conduct an *ex ante* review to confirm that the transferred intelligence would not violate State A's access requirements. State A's authorizer reviews the transferred information and notices a reference to a State A national. The authorizer must then redact the information revealing personal information about the State A national. State A might ask whether the raw intelligence information was collected through bulk surveillance. State B would either have to answer State A's question or not share the bulk data. Assuming that State B explained that the information had been gathered through bulk interception, State A would then need to determine if there were a way by which State A could access the information. While State A might have an absolute rule allowing for no exceptions for bulk interceptions, it also might have a rule that permits access to a targeted subset of the bulk dataset with independent judicial authorization. Thus, State A's domestic legislation would determine State A's ability to access such information. If State A accesses personal information from State B's report, State A must notify State B. State B would then carry out notifications in line with the notification requirements outlined in its domestic legislation. State A would also need to erase the transferred data in accordance to agreed-upon retention limitations.

Unless State A has a separate intelligence sharing agreement with State C, State A would probably not be able to receive information from State C. However, if State A's preexisting intelligence leads them to reasonably believe that a) the plot against State A poses a "high-probability event that reasonably threatens the loss of life or substantial disruption to core operational services,"

and b) State C's intelligence could offer "material information germane to the reduction of the threat;" then State A could request such information from State C. However, any information received by State C under the exigency exception could only be used for the specific threat for which the information was requested.

VI. DEFENSE AGAINST COMMON CRITIQUES

A. *Insufficient Privacy Protection*

The framework above will likely raise some critiques. Most predictable is the critique from the European privacy rights camp, arguing that the proposed framework will allow intelligence sharing of information with lesser privacy protections than are mandated by the European Court of Human Rights. Substantively, this criticism is correct. If one adopts a singular approach where privacy concerns operate as the only valid interest at play, then the above framework would inexcusably disregard fundamental rights. However, such an argument stumbles once one reintroduces a critically absent component: the context. As this Article demonstrates, privacy interests operate in tension with *another fundamental right*. While privacy activists will nominally recognize that their "fundamental" privacy right is not in fact absolute, such recognition is usually just that—nominal. Take for example Hielke Hijmans's *The European Union as Guardian of Internet Privacy.* In one line during his six-hundred page tome, Hijman recognizes that "[t]hreats to security may require restrictions to the exercise of fundamental rights."[294] Even Hijmans's language is striking—"fundamental" rights connote absolute and inalienable qualities. Given the legitimate restriction of these rights, they clearly do not carry an absolute quality. If threats to security warrant the restriction of fundamental rights, then it serves to reason that threats to security also implicate fundamental rights. In short, there is a tradeoff here.

Given the presence of a tradeoff between fundamental rights, privacy advocates' implicit paradigm of "security—bad, privacy—good"

[294] Hijmans, *supra* note 218, at 113–14.

inappropriately misconstrues the moral considerations. By downplaying the human rights interests in adequate security, privacy advocates paint their advocacy for greater privacy protections as a unilateral quest for maximizing human rights. For example, claims proliferate founded upon the assumption that strengthening privacy at the expense of security will lead to "the establishment of a high ceiling rather than a low floor for human rights protection and accountability."[295] Similarly, this blinkered viewpoint leads to characterizations of counterterrorism practices leading to privacy limitations as "[a] race to the bottom concerning the right to privacy."[296] Such pejorative language disparages legitimate security behavior protecting fundamental rights.

The European Union, with support from privacy activists around the world, has staked out the moral high ground, declaring that their desired balance—and none others—deserve consideration or deference. As Maria Tzanou observes, "the EU has successfully constructed the image of itself as a 'moral leader of good in the fight against terrorism due to its alleged higher respect to human rights standards compared to the US."[297] Hijman reports that European Council intentionally sought to set "globalization within a moral framework."[298] Once the privacy-security balance has been 'moralized,' the heart of the question becomes whether states can legitimately strike different balances along this spectrum.

According to the European Union and privacy activists, that answer is no. The European Union has adopted its role on the basis that its values are "normatively desirable and universally applicable."[299] Hijmans provides a helpful descriptor for this practice: "regulatory imperialism."[300] The CJEU has encouraged this path towards European exceptionalism with its decision in *Kadi*: "EU concepts on fundamental rights prevail, whenever this is necessary, over international law. EU law contains principles that must be respected in

---

[295] Brown et al, *supra* note 199.

[296] Tzanou, *supra* note 144, at 101.

[297] *Id.* at 100.

[298] Hijmans, *supra* note 218, at 482–83. https://link.springer.com/content/pdf/10.1007/978-3-319-34090-6.pdf.

[299] *Id*; *see also* Bignami & Resta, *supra* note 97, at 16.

[300] Hijmans, *supra* note 218, at 488.

the international domain, are not negotiable and subject to full review of the EU Courts."[301]

If one believes the European standard offers immutable expressions of absolute morality, then my framework will be troubling. Stephen Schulhofer has explicitly embraced this approach, and strenuously opposes the effort "to find international common ground" because multilateral negotiation would create a more permissive sharing regime that would create, in his morally-infused words, "a race to the regulatory bottom."[302] Of course, for many, a major thrust of this intelligence sharing critique is that currently *no* country provides adequate privacy protections over intelligence transfers—European human rights law just provides the most promising path forward.

The proposed framework compromises on privacy absolutist ideals in a number of ways. First, the framework argues that data access controls as opposed to data collection controls should not prohibit intelligence sharing agreements. The framework also largely defers the content of such access controls to the domestic state. Second, the framework applies a watered-down proportionality test, and does not call for an independent necessity test. Instead, it would allow legitimate government intelligence requests without an inquiry or adjudication into alternative pathways for acquiring such information. Third, it does not require governments to authorize whistleblowing to the general public. Fourth, it provides for state-notification and does not mandate individual notification. Fifth, it does not demand an individual right of action. Nevertheless, the adoption of such a framework would pose a major step forward for privacy rights by legislating overdue transparency and oversight in a field long obscured by a foggy ether.[303]

Privacy concerns animated by domestic surveillance practices are also mitigated in intelligence sharing. As Schulhofer notes, "US data-collection programs pose a far greater risk of chilling political dissent within the US than of chilling political activity by Germans or Canadians critical of their own

---

[301] *Id.* at 473.

[302] Schulhofer, *supra* note 51, at 240.

[303] This framework also does not discuss control of voluntary disclosures by Internet Service Providers, an area that warrants further analysis in the future.

governments."[304] While foreign governments are less likely to respect an individual's privacy interests, they also have limited means to suppress rights abroad. Thus, to the extent that intelligence sharing serves to provide data on foreigners, some privacy concerns are diminished.[305]

Additionally, the flexibilities of this approach make this framework practicable. The framework governs intelligence sharing practices yet places a light touch on the surveillance methods employed in each country. Privacy idealists too often ignore that a failure to grant intelligence operations special treatment will result in widespread noncompliance.[306] After all, law as practiced within the "real world" context— operating under an operational code—are viewed as lawful by those operators.[307] This remains true even when those operational laws deviate from the established myth system.[308] Following Asaf Lubin's lead, this Article urges a practical orientation that would shatter the "Geneva echo chamber" and reintroduce government stakeholders into the discussion.[309] Furthermore, while some might find attractive the notion of disregarding foreign balances, the reality is that "countries with different values, . . . for instance, the BRICS countries[310] are gaining more economic power."[311] The BRIC countries are not only growing in economic power, but many also have extensive intelligence apparatuses.

---

[304] Schulhofer, *supra* note 51, at 260.

[305] This is not to say that information sharing does not cause any privacy harm. Many of the privacy concerns outlined in Part 0 still apply.

[306] *See* Deeks, *supra* note 63, at 602 ("The formalists ignore that there is something unique about intelligence activity, and that requiring intelligence services to play by precisely the same rules as law enforcement, diplomatic, and military actors is doomed to produce state noncompliance.").

[307] Lubin, *supra* note 51, at 511 (citing W. Michael Reisman, *Myth System and Operational Code*, 3 YALE STUD. WORLD PUB. ORD. 229, 230 (1977)).

[308] *Id.*

[309] *Id.* at 551–52 ("This piece proposes recognizing the legitimacy behind certain limited legal differentiations in treatment for domestic and foreign surveillance. Such recognition, quite a concession on the part of the 'Geneva echo chamber,' would bring government agencies back to the table.").

[310] *See BRIC*, CAMBRIDGE DICTIONARY, https://dictionary.cambridge.org/us/dictionary/english/bric (last visited Mar. 13, 2019) (referring to the economic pact comprised of Brazil, Russia, India and China).

[311] Hijmans, *supra* note 218, at 459.

These countries are developing the economic strength to withstand regulatory imperialism, and the need for information sharing means that their interests cannot simply be ignored. In short, this paper incorporates flexibilities, and by doing so, promulgates standards that could actually work.

B. Undermines Democratic Accountability

A similar critique suggests that an international framework undermines democratic accountability. Contrary to these complaints, this international framework will strengthen the role of civil society in holding governments accountable. Some activists have suggested that any international privacy sharing agreement would "sideline the courts, disempower legislative bodies and privacy advocates, defuse commercial pressure for strong privacy safeguards, and create a dynamic controlled almost exclusively by the executive and its national security establishment."[312] However, this fear ignores the limited control that civil society currently exerts—intelligence sharing remains a black box. By bringing (more) sunshine to the shadows of intelligence cooperation, privacy activists will receive the benefit of pushing standards and accountability into these practice areas. Even more importantly, the intelligence-sharing framework furthers transparency in far less privacy-sympathetic regimes, thereby providing an avenue for civil society to make further inroads on government accountability.

C. International Agreements Are Unrealistic

Many scholars view the notion of any international information-sharing regime as a fanciful one. While proposing international agreements might be an attractive theoretical exercise, many question the practical utility of pushing for "an international treaty forged out of pixie dust."[313] In other words, even if one accepts the principles outlined under the proposed framework, states would never agree to an international treaty. Academics provide many reasons for their skepticism: varying privacy commitments, foreign mistrust, and state sovereignty concerns.

---

[312] Schulhofer, *supra* note 51, at 240.

[313] Woods, *supra* note 59, at 781.

i. Irreconcilable Ideological Differences

Doubters suggest that states' different privacy-security balances pose an insuperable barrier to intelligence sharing. This perspective posits a "probably unbridgeable-gulf" between different states' commitment to privacy protection.[314] As one skeptic reports, "There is absence of global consensus at an aspirational level, in particular, where this approach implies agreement with countries that do not share basic democratic values."[315]

Another suggests that an international agreement "will necessarily be based on a lowest common denominator."[316] These realists are correct to recognize the different surveillance standards across countries, and an attempt to coerce all states to a uniform practices would not succeed. The proposed framework recognizes this ideological reality, and grants states significant discretion in the ways that they carry out intelligence work. Instead of prescribing an ideological viewpoint, the framework sidesteps these unyielding ideological positions by requiring unobjectionable procedural processes that facilitate the unifying interest in accessing critical intelligence.

ii. Too Much Foreign Mistrust

Another critique dismisses an intelligence-sharing agreement as unattainable due to an insufficient level of popular trust. While citizens might submit to some degree of surveillance by their own government, they would not necessarily agree to similar oversight by foreign entities. As one observer put it, "Brits may have become used to the CCTV cameras and Automatic Number Plate Recognition technology that allows their own government to monitor their travel – but they would be considerably more dubious about letting the Germans and the French do the same."[317] While some citizens will

---

[314] *See* Schulhofer, *supra* note 51, at 254 (asserting that, notwithstanding existing frameworks between the United States and other Western states, "the complexity of the issues and the diametric opposition" ensure that progress "will be arduous and slow").

[315] Hijmans, *supra* note 218, at 491.

[316] *See* Woods, *supra* note 59, at 788.

[317] Robin Simcox, *Europe, Stop Trying To Make 'Intelligence Sharing' Happen*, FOREIGN POL'Y (Apr. 14, 2016, 3:19PM), http://foreignpolicy.com/2016/04/14/europe-stop-trying-to-mak-brussels-paris-bombings.

undoubtedly find this scope unsettling, this discomfort would not likely pose a practical barrier. This is the case for several reasons. First, the procedural safeguards significantly reduce the degree of the privacy harm. States can only share information under heavily prescribed circumstances. The fact that only foreign intelligence officials can access the information would also significantly diminish citizen reticence. The average citizen is unlikely to fear that he or she will be a subject of a foreign national security investigation. As a result, most citizens will not see this law as impacting their lives. Moreover, the notification regime requiring home states to notify individuals whenever foreign intelligence agencies access their private information will further mollify citizen concerns. In short, the intelligence-sharing framework sufficiently curtails citizens' privacy risks to avoid popular resistance.

iii. Compromises State Sovereignty

Another critique questions this framework as hobbling state sovereignty. According to this argument, national governments will not submit to an agreement that limits their ownership over their privacy-security balance. Instead of the domestic national legislature determining the appropriate level of privacy intrusion, foreign states violate that national compact through sharing intelligence collected through different standards. This would be a legitimate concern, were it not for the presence of access controls. Through the exercise of access controls, states maintain control over their intelligence agencies' acceptable practices. Relatedly, it true that this framework facilitates intelligence sharing with foreign states that do not necessarily subscribe to the same privacy standards. However, it would be a mistake to consider intelligence sharing as diminishing state sovereign control. As Jennifer Daskal points out, "[T]his critique assumes a world that does not exist. It assumes that foreign governments will comply with the existing diplomatic procedures for accessing sought-after data rather than seeking out means of accessing the data unilaterally."[318] In the absence of intelligence agreements, foreign intelligence agencies would attempt to gather the same intelligence information by sweeping and privacy-invasive collection of raw data. By

[318] Daskal, *supra* note 50, at 497.

developing procedural limitations for the use of shared intelligence that render such invasive tactics less necessary, states reduce the incentive for costly foreign surveillance efforts. Therefore, the intelligence framework would likely allow states to exercise far *greater* sovereign control over the shared information.

Others argue that state national security branches have little interest in allowing any further limitations on their near-absolute discretion over intelligence practices. In other words, government officials have a strong interest in maintaining the status quo. However, this approach overlooks the changing norms leading to a public expectancy of greater transparency over intelligence activities.[319] Even those countries that do not face public pressure are indirectly impacted by this normative trend. The push for government accountability has jeopardized the ability for other states to receive foreign intelligence. Given the collective interest—and need—for intelligence sharing, governments have an interest in adopting procedural practices that will allow for intelligence sharing without compromising their national intelligence practices. Sovereign states enter international agreements that they view in their national interest, and adopting this framework promotes vital security interests.

VII. PATHWAYS TO IMPLEMENTATION

The proposed framework benefits from multiple avenues towards implementation. The first option is through unilateral, domestic legislation. Unlike many areas of the anarchic international arena, no collective action problem prevents unilateral adoption by individual states. As the public eye increasingly scrutinizes intelligence practices and calls for intelligence reform, states will also experience unprecedented constraints on intelligence sharing at a time when such sharing has never been more vital. The CJEU decisions in *Schrems* and *Canada PNR*[320] are only the tip of the iceberg. As states fill out their surveillance jurisprudence, they will continue to proliferate incompatible

[319] Deeks, *supra* note 63, at 618 ("Overall, the public now expects greater transparency about intelligence activities and some governments have begun to provide it.")

[320] *See* Opinion 1/15, ¶ 1, ECLI:EU:C:2017:592.

sharing regimes. Rather than continue their collision course with other privacy regimes, states can adopt these proposed procedures. As detailed above, states can adopt these procedures with minimal cost to their preferred privacy-security balance.

In order to be maximally effective, states would want to adopt these regulations with their closest intelligence allies. Fortunately, preexisting cooperation abounds. As Orin Kerr reports, "A complex web of global, regional, and bilateral treaties now exists addressing a wide range of crimes, such as cybercrime, corruption, transnational organized crime, narcotics, and terrorism."[321] Nations have already adopted information-sharing agreements through MLATs[322] and through financial intelligence cooperation.[323]

Bilateral agreements also provide a promising approach. A small core of states pushing this framework through bilateral agreements could quickly lead to sustained momentum. The Group of Eight (G8) countries—made up of France, Germany, Italy, the United Kingdom, Japan, the United States, Canada, and Russia might be one place to start. The G8 already has a history of coordinating regulatory efforts of a series of internet-related crimes, including industrial and state espionage.[324] The G8 states' extensive intelligence capabilities grant this group exceptional influence over promoting

---

[321] Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. 58, 61 (2017).

[322] *See* primer discussion on the United States' use of MLAT agreements, *supra* note 13.

[323] Mara Lemos Stein, *The Morning Risk Report: Financial-Intel-Sharing Groups Need Diversity*, WALL ST. J.: RISK & COMPLIANCE J. (Jan. 10, 2018, 7:32 AM), https://blogs.wsj.com/riskandcompliance/2018/01/10/the-morning-risk-report-financial-intel-sharing-groups-need-diversity; see also *International Programs*, U.S. DEP'T TREASURY: FINANCIAL CRIMES ENFORCEMENT NETWORK, https://www.fincen.gov/resources/international-programs (last visited Oct. 11, 2018) ("FinCEN is one of the most active FIUs in the world in terms of exchanging information with counterpart FIUs. The demand for FinCEN's services from foreign FIUs has expanded dramatically over the past decade.").

[324] Ghappour, *supra* note 159, at 1131 (citing Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 147 (2000)).

such a framework.[325] This could arise through an informal agreement, or even the development of a multinational institution.

Financial intelligence cooperation shows the promise of such an approach. The effort to promote financial intelligence exchange has led to the development of a distinct international institution, the Egmont Group, comprised of 155 Financial Intelligence Units.[326] Egmont has played a role in responding to terrorist financing and provided a secure technological platform for financial intelligence exchange.[327] The long-term establishment of such an organization could help reduce information costs of monitoring intelligence-sharing which states have legislated sufficient procedural safeguards.

Formal international treaties offer another way forward. These agreements can move through the United Nations, which some have argued presents "the legitimate forum for the negotiation of a global legal framework."[328] However, others have argued that adopting an international agreement would trade efficiency for a cumbersome process that could prolong and delay adoption of new domestic legislation.[329] Nevertheless, formal international agreements could clarify the specific elements of the framework and ensure that all states are applying the same framework. As intelligence sharing becomes a more regulated practice, a treaty might help codify a widespread state practice. At this time, such an approach would likely be premature.

---

[325] American data providers' dominance over the global market gives the United States in particular tremendous leverage in facilitating an intelligence-sharing regime. *See* Daskal, *supra* note 51, at 474.

[326] *About*, EGMONT GROUP, https://egmontgroup.org/en/content/about (last visited Oct. 11, 2018).

[327] Egmont Group, Group of Financial Intelligence Units, Annual Report 2015–2016 11 (2017), https://egmontgroup.org/en/filedepot_download/1660/45.

[328] Report on the meeting of the Expert Group to Conduct a Comprehensive Study on Cybercrime, UNODC/CCPCJ/EG.4/2017/4, ¶43 (Apr. 24, 2017), http://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/Cybercrime_report_2017/Report_Cyber_E.pdf.

[329] Koops & Goodwin, *supra* note 32, at 83..

VIII. CONCLUSION

In the early 21st century, the international community remains comprised of independent, sovereign nation states. These sovereign states will choose different privacy security tradeoffs. Governments will need to navigate a way to maintain intelligence sharing in an age when government surveillance receives increasing scrutiny. As one British parliamentarian aptly articulated, "We need to face up to the challenge —not duck, ignore, or pretend it is not there—[t]o preserve the legal safeguards that ensure that our intelligence services can do their job."[330]

The proposed intelligence framework offers a road forward; one that respects sovereign choices and also comports with international law. The proposed intelligence framework is practicable and promises unprecedented transparency in an area long devoid of legal governance. Countries implementing this framework would create unparalleled democratic accountability, without undermining intelligence officials' ability to do their jobs. Governments will be able to keep people safe and also provide meaningful privacy protection. As privacy activists demand greater transparency on intelligence sharing, both governments and privacy advocates should consider this framework as a compromise path forward. In short, this framework empowers countries to transform the impending clash of privacy-security regimes into an opportunity for a new era of global cooperation and transparency.

---

[330]15 Mar. 2018, Parl. Deb HC (2018) col. 158, https://hansard.parliament.uk/commons/2018-03-15/debates/831521d4-174f-4150-9099-7817a9e28f8b/DataProtectionBill (click PDF and HTML downloads; select "Data Protection Bill [Lords] (Fourth sitting)).