VIRGINIA LAW REVIEW

VOLUME 106 NOVEMBER 2020 NUMBER 7

ARTICLES

SECRECY SURROGATES

*Ashley Deeks**

Debates about how best to check executive branch abuses of secrecy focus on three sets of actors that have access to classified information and that traditionally have served—in one way or another—as our surrogates: congressional committees, federal courts, and leakers or whistleblowers. These actors provide only limited checks on the Executive's misuse of secrecy, however. Most legal scholarship bemoans their flaws but concludes that the status quo is the best that we can do. This Article challenges this account, arguing that there is a different set of actors—a set of unsung "secrecy surrogates"—that can provide additional checks on the quality and legality of the Executive's classified operations in the cyber, election, and counter-terrorism settings.

Technology companies, states and localities, and foreign allies have become an integral part of U.S. national security operations and enjoy some critical advantages over our traditional surrogates. These actors possess expertise about—and in some cases control—national security-related targets, making them essential partners for the Executive. Further, these surrogates have incentives to check the Executive in ways that advance the public law values of accuracy, accountability,

* Professor, University of Virginia Law School. Thanks to George Cohen, Jen Daskal, Kristen Eichensehr, Mike Flowers, John Harrison, Debbie Hellman, Rebecca Ingber, Nate Jones, Aaron Karczmer, Matt Olsen, Daphna Renan, Rich Schragger, Paul Stephan, and participants in the 2019 Duke-Virginia Foreign Relations Roundtable and in workshops at Harvard Law School and the University of Houston Law Center for very helpful conversations and comments.

and legality. Finally, unlike leakers, these unsung secrecy surrogates can challenge the Executive without revealing government secrets. These surrogates can only check government abuses of secrecy as long as the Executive requires their cooperation, but they have begun to supplement our traditional surrogates in important ways.

This Article maps the growing role of these unsung secrecy surrogates, argues that they are well-situated to address some persistent secrecy problems, and proposes ways to preserve and enhance the surrogates' position in the secrecy ecosystem in the future.

INTRODUCTION

Misuse of government secrecy is in the headlines. Consider the revelation that White House officials transferred the transcript of President Trump's call with Ukraine's President to a highly classified stand-alone computer system to prevent leaks.[1] For many, this incident reflects a paradigmatic problem with government secrecy: actors in the Executive can employ it as a tool to avoid politically embarrassing or legally problematic revelations.[2] This episode proved to be a success story. A government whistleblower carefully followed statutory procedures, and the Intelligence Community Inspector General shared the

[1] Julian E. Barnes, Michael Crowley, Matthew Rosenberg & Mark Mazzetti, White House Classified Computer System Is Used To Hold Transcripts of Sensitive Calls, N.Y. Times (Sept. 29, 2019), https://www.nytimes.com/2019/09/27/us/politics/nsc-ukraine-call.html [https://perma.cc/F9ZC-68Z3]; see Dustin Volz, Andrew Duehren & Natalie Andrews, White House Official Feared Trump Transcript Leak Could Be Politically Damaging, Wall St. J. (Nov. 17, 2019, 5:52 AM), https://www.wsj.com/articles/white-house-official-feared-trump-transcript-leak-could-be-politically-damaging-11573942481 [https://perma.cc/LV53-PL42].

[2] See, e.g., Ayesha Rascoe & Franco Ordoñez, Former Officials Say White House's Use of Secret System Is Unusual, 'Disturbing,' NPR (Sept. 27, 2019, 5:40 AM), https://www.npr.org/2019/09/27/764759182/former-officials-say-white-houses-use-of-secret-system-is-unusual-disturbing [https://perma.cc/7PBJ-5MF8] (quoting former White House official as stating that "[t]his seems to be nothing more than an abuse of the classification and the information security system to safeguard not the information, but to effect a cover-up" (internal quotation marks omitted)).

whistleblower's complaint with Congress, which held impeachment hearings to judge the President's actions. Yet the case may be just as notable for its uniqueness, given how infrequently the whistleblowing process works as intended.

Indeed, legal scholars and political scientists have long decried the current state of affairs, in which the Executive exercises near total control over secret government information with few external checks. A substantial literature wrestles with how to manage the genuine need for secrecy about many national security operations in a democracy whose government should be accountable to the people. Government secrecy can foster four types of problems. First, the Executive can employ secrecy to conceal unlawful acts, such as spying on political enemies. Second, the Executive can use secrecy to conceal poor or controversial judgments or policies. Third, the Executive can use secrecy to conceal incompetent, empirically wrong, or insufficient intelligence and analysis.[3] Each of these three types of missteps is embarrassing to the Executive and creates incentives to conceal the underlying action.[4] Fourth, making decisions in secret insulates the Executive from having to justify and defend those decisions in public.[5] All of these possible abuses of secrecy engender public skepticism about the government and make it harder for the

[3] See Loch K. Johnson, Governing in the Absence of Angels: On the Practice of Intelligence Accountability in the United States, *in* Who's Watching the Spies? Establishing Intelligence Service Accountability 57, 61 (Hans Born, Loch K. Johnson & Ian Leigh eds., 2005) (quoting intelligence scholar as stating that the major problem facing U.S. intelligence in 2005 was that the "CIA [had] not been gathering enough quality data").

[4] See Frederick A.O. Schwarz Jr., Democracy in the Dark: The Seduction of Government Secrecy 2 (2015) ("[T]oo much is kept secret not to *protect America* but to keep embarrassing or illegal conduct *from Americans*.").

[5] Robert M. Pallitto & William G. Weaver, Presidential Secrecy and the Law 3 (2007) (noting executive interest in "maintain[ing] presidential prerogative against congressional inquiries and judicial orders"); id. at 6 ("Where a president may do what is desired in secret, there is no reason to withstand the ordeal of a political battle to achieve the same ends."); H.R. Select Comm. To Investigate Covert Arms Transactions with Iran & S. Select Comm. on Secret Military Assistance to Iran and the Nicaraguan Opposition, 100th Cong., Rep. of the Congressional Committees Investigating the Iran-Contra Affair, Minority Report 450, 515 (Comm. Print 1987) (stating that the President should undertake "democratic persuasion" to develop support for his policies and that he will not succeed "unless the public is exposed to and persuaded by a clear, sustained, and principled debate on the merits"); David E. Pozen, Deep Secrecy, 62 Stan. L. Rev. 257, 279 (2010) (discussing how secrecy provides "insulation from scrutiny").

public—and U.S. allies—to trust the Executive in cases in which secrecy truly is necessary.[6]

Legal scholarship about government secrecy usually focuses on three sets of actors that check and balance executive branch secrecy to reduce abuse.[7] Two sets of actors lie in the Executive's co-equal branches of government. In the 1970s, Congress created two intelligence committees—the Senate Select Committee on Intelligence ("SSCI") and the House Permanent Select Committee on Intelligence ("HPSCI")—in the wake of the Church and Pike Committees' reports. The intelligence committees, which conduct much of their work in secret, directly oversee the intelligence community and its activities.[8] The 1970s reforms also produced the Foreign Intelligence Surveillance Court, in which Article III judges authorize executive surveillance for foreign intelligence purposes. Article III courts also review classified information and activities in cases involving state secrets, Freedom of Information Act litigation, and certain criminal cases.

Although not constitutionally linked to the public in the way that Congress and federal courts are, whistleblowers and leakers constitute a third set of actors who attempt to bring abuses (or alleged abuses) to the

[6] See Pozen, supra note 5, at 280; S. Select Comm. To Study Governmental Operations with Respect to Intel. Activities, Final Report, S. Rep. No. 94-755, at 4 (1976) ("[T]here are many necessary and proper governmental activities that must be conducted in secrecy. . . . [However,] intelligence activities conducted outside the framework of the Constitution and statutes can undermine the treasured values guaranteed in the Bill of Rights. Further, if the intelligence agencies act in ways inimical to declared national purposes, they damage the reputation, power, and influence of the United States abroad.").

[7] See, e.g., Rahul Sagar, Secrets and Leaks: The Dilemma of State Secrecy (2013) (considering role of Congress, the courts, whistleblowers, and leakers in managing government secrecy); Pallitto & Weaver, supra note 5 (considering Congress, the courts, and leaks); Michael P. Colaresi, Democracy Declassified: The Secrecy Dilemma in National Security 181 (2014) (discussing role of legislatures, freedom of information laws, and press freedom laws in checking executive secrecy); Mark Fenster, The Transparency Fix: Secrets, Leaks, and Uncontrollable Government Information (2017) (discussing the role of the press, freedom of information laws, anti-corruption non-governmental organizations, and leaks); Pozen, supra note 5, at 269, 274 (focusing on deep secret keeping by executive officials, treating Congress and the courts as the primary recipients of shallow secrets, and assuming that very few private actors generally will be aware of government secrets); Johnson, supra note 3, at 58 (noting that the "most consistent and serious manifestation of intelligence oversight has come not from presidential commissions, but from the media and the Congress"); Josh Chafetz, Whose Secrets?, 127 Harv. L. Rev. F. 86, 87 (2013) (emphasizing the role of Congress in the secrecy regime).

[8] Members of the committees that oversee military and foreign relations issues also have access to classified information relevant to their legislative and oversight tasks.

attention of actors outside the Executive. In the national security setting, leakers emerge from within the executive branch itself and usually remain anonymous. They reveal classified information to the public, often by sharing it with journalists who report on the programs or intelligence contained in the leak. Whistleblowers, on the other hand, follow a statutory process of revealing abuses to their agency's inspector general and then potentially to members of Congress.

Some view these three sets of actors as surrogates for the broader public, which does not and often should not have access to government secrets. As the literature makes clear, however, all three groups are imperfect surrogates. Congressional committees lack the robust incentives and sometimes the deep experience necessary to check the Executive's national security activities. Federal courts often doubt their own competence to evaluate secret government programs and so accord substantial deference to executive claims that certain disclosures will harm national security. Leakers reveal information sporadically and can harm genuine national security equities when they do so. Leaking classified information also generally violates criminal law. And whistleblowing is fraught: those who blow the whistle often are subject to retaliation, even though statutes prohibit such responses.

Notwithstanding the flaws in the capabilities and performance of these three groups, many have concluded that the current state of affairs is the best we can do. This Article challenges that conclusion, arguing that this model overlooks at least three other sets of actors who increasingly can and do play a role in curbing misuses of executive secrecy.[9] In recent decades, the national security threat landscape has shifted from one of overt, kinetic state-to-state conflict to a landscape dominated by non-state actors and clandestine, hostile operations by foreign governments using new technologies. In light of these new threats, which manifest themselves in the form of pernicious cyber operations, election interference, and terrorist acts, three groups have assumed critical—though underappreciated—roles in the U.S. national security ecosystem.[10]

[9] I have argued elsewhere that other actors and mechanisms constrain the Executive in its classified operations, including executive branch lawyers and norms of reason giving. See Ashley Deeks, Checks and Balances from Abroad, 83 U. Chi. L. Rev. 65 (2016) [hereinafter Deeks, Checks and Balances]; Ashley S. Deeks, Secret Reason-Giving, 129 Yale L.J. 612 (2020) [hereinafter Deeks, Reason-Giving]; Ashley S. Deeks, The Substance of Secret Agreements and the Role of Government Lawyers, 111 AJIL Unbound 474 (2018).

[10] Additional actors play a role in what this Article terms the "secrecy ecosystem." These actors include the Privacy and Civil Liberties Oversight Board, the Presidential Intelligence

U.S. technology companies,[11] states and localities, and foreign allies all possess the capacities and incentives to check problematic uses of government secrecy. For example, technology companies exchange threat information and operational details of cyber attacks with government officials, comparing intelligence and sometimes litigating to contest government decisions to keep programs secret.[12] Foreign allies sometimes

Advisory Board ("PIAB"), and the Defense Advisory Board. See, e.g., Kenneth Michael Absher, Michael C. Desch & Roman Popadiuk, Privileged and Confidential: The Secret History of the President's Intelligence Advisory Board (2012) (discussing the PIAB); Johnson, supra note 3, at 73 (noting that when Brent Scowcroft was Chair of the PIAB, he produced a "hard-hitting review" of the intelligence organization). For reasons of space, however, this Article does not address the role of these other secrecy surrogates.

[11] By "technology companies," I mean large social media, software, and computer technology companies such as Google, Microsoft, and Facebook, as well as companies that provide cybersecurity services, such as FireEye/Mandiant, Crowdstrike, and IronNet.

[12] Similar interactions conceivably occur with utility companies and private banks because these companies have been targets of thousands of hostile cyber operations. The Intelligence Community's 2019 Threat Assessment noted, "Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016." Daniel R. Coats, Dir. of Nat'l Intel., Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community 6 (2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf [https://perma.cc/M7DS-WPY4]. Further, the Intelligence Community is authorized to disseminate "classified reports to critical infrastructure entities authorized to receive them." Off. of the Dir. of Nat'l Intel., Dep't of Homeland Sec., Dep't of Def. & Dep't of Just., Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government Under the Cybersecurity Information Sharing Act of 2015, at 13 (2016), https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_(103).pdf. [https://perma.cc/HYH7-XUCD]. This Article focuses on technology companies because they are most likely to be sophisticated consumers (and providers) of intelligence on cyber operations. Some utility companies are reportedly insufficiently focused on cybersecurity and thus are poorly positioned—at least right now—to play a significant role in checking a sophisticated actor like the Executive. For a critique of utility company cybersecurity practices, see Joseph Marks & Tonya Riley, The Cybersecurity 202: Activist Wants Court To Name and Shame Electric Utilities for Violating Cybersecurity Rules, Wash. Post (Dec. 3, 2019, 4:35 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/12/03/the-cybersecurity-202-activist-wants-court-to-name-and-shame-electric-utilities-for-violating-cybersecurity-rules/5de550bf88e0fa652bbbdb18/ [https://perma.cc/N43C-Z4ZL]; Catherine Stupp, Utilities Are Prime Targets for Cyberattacks, WSJ Pro Cybersecurity (Aug. 7, 2019, 11:19 AM), https://www.wsj.com/articles/utilities-are-prime-target-for-cyberattacks-11565170204 [https://perma.cc/2S5J-EJU6] ("Utilities often don't have enough employees with security clearance that lets them quickly get classified information about cyber threats from the federal government."). Utilities, banks, and other operators of critical infrastructure may play a greater checking function in the future as they gain more experience with these threats. For a report recommending that the government enhance its sharing of classified information with utilities grid operators, see Nat'l Comm'n on Grid Resilience, Grid

disagree with the U.S. intelligence community's substantive intelligence judgments, challenging the United States to produce more or better intelligence.[13] Although there are limited public examples of states and localities challenging secret executive activities directly in the election and cyber arenas, these sub-federal officials have the potential to do so because they possess fine-grained information about the election systems and critical infrastructure that are the targets of hostile cyber operations.[14] Further, they historically have challenged certain federal counter-terrorism programs, which suggests that they may start to push back in the election and cyber settings as they gain expertise about the threat landscape.[15]

These three groups have several important advantages over our traditional secrecy surrogates. First, they possess *specific expertise* about the new threats and new targets that Congress, the courts, and leakers might not. Certain technology companies and many allies are highly specialized in intelligence-gathering and analysis, and so are particularly well-suited to detect problematic executive performance in the secrecy space.[16] Second, each of the three groups brings to the table *irreplaceable*

Resilience: Priorities for the Next Administration 28 (2020), https://gridresilience.org/wp-content/uploads/2020/08/NCGR-Report-2020-Full.pdf [https://perma.cc/5QMV-XUAN].

[13] For example, the Trump Administration has tried for more than a year to persuade allies not to employ Huawei equipment in their 5G networks and has received pushback from a range of foreign governments. Robbie Gramer & Lara Seligman, Can the U.S.-U.K. Special Relationship Weather the Huawei Storm?, Foreign Pol'y (Jan. 30, 2020, 5:10 PM), https://foreignpolicy.com/2020/01/30/huawei-intelligence-united-states-britain-trump-5g-in-frastructure-concerns-digital-espionage-special-relationship-five-eyes/ [https://perma.cc/7Z-48-TKWX].

[14] For instance, in 2013, Los Angeles created a Cyber Intrusion Command Center, City of Los Angeles, Exec. Directive No. 2 (Oct. 30, 2013), https://www.lamayor.org/sites/g/files/wph446/f/page/file/ED2_with_signature_and_letterhead.pdf?1426620047 [https://perma.cc/6E9C-JC7M] (anticipating collaboration with the FBI and other federal agencies), and in 2017, New York City created its own Cyber Command, City of New York, Exec. Order No. 28 (July 11, 2017), https://www1.nyc.gov/assets/home/downloads/pdf/executive-orders/2017/eo_28.pdf [https://perma.cc/7CNG-HAMH] (anticipating collaboration with federal and state government agencies and the private sector); see also Brennan Weiss, Inside New York City Cyber Command, Bus. Insider (May 5, 2018, 8:00 AM), https://www.businessinsider.com/nyc-cyber-command-protecting-new-yorkers-2018-4 [https://perma.cc/46VA-MWC7].

[15] See Matthew C. Waxman, National Security Federalism in the Age of Terror, 64 Stan. L. Rev. 289, 333 (2012).

[16] A possible analogy is to the role of auditors, who verify the accuracy of the government's records (here, its intelligence and analysis) and point out deficiencies in its operations. For the use of the concept of substantive audits in the intelligence setting, see Eric Posner, It's Time to Audit America's Secrets, Foreign Pol'y (Feb. 2, 2018,

access to information and infrastructure that the Executive needs to perform its job.[17] For technology companies, it is the ability to observe and defend the front lines of critical infrastructure systems, attribute the sources of cyber attacks, and operate the very systems that are subject to foreign manipulation. For states and localities, it is control over and knowledge about election operations and machinery (and other critical infrastructure at the sub-federal level), as well as ground-level intelligence about terrorist activities inside the United States. For foreign allies, it is intelligence and expertise that the United States may not possess about shared threats. The Executive has persistent incentives to share intelligence with these actors to allow them to take necessary steps to enhance U.S. national security. This, in turn, renders them an audience that the Executive must persuade of the soundness of its intelligence and proposed operations.[18] Third, unlike leakers, these three groups are positioned to challenge secret government operations *without revealing those operations*.[19]

These, then, are our unsung "secrecy surrogates": actors who are given access to secret information that average U.S. citizens are not and who can improve secret executive operations and help mitigate abuses. By "surrogates," I do not mean that these groups have a direct constitutional, contractual, or agency relationship with the national populace—they generally do not.[20] Instead, I mean that these groups serve as our surrogates in a more general sense: as actors who take our place or are

5:13 PM), https://foreignpolicy.com/2018/02/02/its-time-to-audit-all-of-americas-secrets/ [https://perma.cc/LK65-W4NA]; Elizabeth Goitein & J. William Leonard, Opinion, America's Unnecessary Secrets, N.Y. Times (Nov. 7, 2011), https://www.nytimes.com/2011/11/07/opinion/national-security-and-americas-unnecessary-secrets.html [https://perma.cc/2UAL-GFKL] (arguing that one way to combat government over-classification is to allow agencies' inspectors general to "audit officials' classification decisions").

[17] See Michael Wines, State Officials Say They Are Told Too Little About Election Threats, N.Y. Times (Feb. 19, 2018), https://www.nytimes.com/2018/02/19/us/elections-states-hacking.html [https://perma.cc/77LU-KFCV] (describing the relationship between the Department of Homeland Security and local election officials as an "arranged marriage").

[18] Deeks, Reason-Giving, supra note 9.

[19] Those who frame the government secrecy debate as a choice between secrecy and disclosure thus are misframing the issue. See Philip H. Melanson, Secrecy Wars 8, 183 (2001) (describing the "ongoing battle between secret keepers and those seeking access").

[20] There is an irony here: in certain areas of classified government operations, these actors, which lack a constitutional relationship to our national polity, may be better positioned to alter the non-public behavior of the Executive than the courts and congressional committees, which are our direct surrogates.

given a particular role in government operations because we are not able to serve in that role ourselves. In particular, these surrogates are positioned to enhance the Executive's adherence to public law values by (1) stimulating the Executive to improve the accuracy of its intelligence; (2) diminishing the Executive's opportunity to undertake illegal actions; and (3) increasing the Executive's accountability for its classified choices.[21] It is difficult to obtain empirical, unclassified information about the full range of effects of these secrecy surrogates, and so this Article's conclusions are necessarily tentative. However, based on available analyses of the ways that technology companies, foreign allies, and states and localities have behaved to date in the surveillance,[22] cybersecurity,[23] and counter-terrorism[24] settings, it is clear that these actors can help ensure that U.S. intelligence operations are attentive to legal, procedural, and accuracy concerns and have begun to play this role.

David Pozen has argued that it is preferable in a democratic system like ours, in which the government must keep certain information secret, for those secrets to be shallow rather than deep. (By deep secrets, he means government secrets that only a small number of similarly situated officials know.)[25] In his view, which I share, our system should favor shallow secrecy whenever possible, because doing so "will systematically lead to . . . outcomes that are deemed acceptable from a greater variety of perspectives, that have been more thoroughly reasoned and refined through a dialogic vetting process, that are better documented, that take

[21] See Jody Freeman, Private Parties, Public Functions and the New Administrative Law, 52 Admin. L. Rev. 813, 818–19 (2000) (listing "openness, fairness, participation, consistency, rationality, impartiality, and accessibility of judicial review" as well as accountability and legality as public law values); id. at 819 ("Private actors are not just rent-seekers that exacerbate the traditional democracy problem in administrative law; they are also regulatory resources capable of contributing to the efficacy and legitimacy of administration."); Michael Taggart, The Province of Administrative Law Determined?, *in* The Province of Administrative Law 1, 3 (Michael Taggart ed., 1997) (defining public law values to include openness, participation, accountability, honesty, and rationality); Mark Aronson, A Public Lawyer's Response to Privatisation and Outsourcing, *in* The Province of Administrative Law 40, 43 (Michael Taggart ed., 1997).

[22] Alan Z. Rozenshtein, Surveillance Intermediaries, 70 Stan. L. Rev. 99, 106 (2018).

[23] Kristen E. Eichensehr, Public-Private Cybersecurity, 95 Tex. L. Rev. 467, 471 (2017) [hereinafter Eichensehr, Public-Private Cybersecurity].

[24] Waxman, supra note 15.

[25] Pozen, supra note 5, at 274 ("[A] government secret is deep if a small group of similarly situated officials conceals its existence from the public and from other officials, such that the outsiders' ignorance precludes them from learning about, checking, or influencing the keepers' use of the information.").

longer to be finalized, and that are more likely to be publicized."[26] He argues that we can shift a secret from being deep to shallow by expanding the number and types of people who know the secret, even if the underlying information remains classified. Pozen, however, contemplates this as occurring primarily by expanding the number and type of secret keepers within the executive branch itself, as well as within Congress.[27] This Article argues that the Executive has, by necessity, begun to expand and diversify the number and type of secret keepers in areas that reach far beyond the executive branch or Congress. In so doing, the government is both decreasing the depth of its secrets and positioning these actors to check some of the persistent problems of government secrecy: the concealment of incompetent execution or illegality and the ability of the Executive to avoid justifying its decisions to outsiders.

This new system of surrogates, like the existing one it supplements, is imperfect. For many of the same reasons that our traditional secrecy surrogates do not act as fully faithful agents for the public, these secrecy surrogates offer only partial fixes to our secrecy challenges, even if they are independently powerful actors.[28] They have their own pathologies and policy preferences, have incomplete access to classified information, and could serve as a new source of leaks. These actors will not supplant the existing messiness of today's interplay among the Executive, Congress, the courts, and leakers. Rather, they will supplement the reach of existing surrogates, expanding what Jack Goldsmith has framed, in the wider national security setting, as a "synopticon"—a distributed network of actors that surveils the Executive.[29] This Article argues that adding knowledgeable players to the "secrecy synopticon" who can provide

[26] Id. at 275.

[27] Id. at 329–30, 333.

[28] Several scholars have considered government secrecy problems through a principal-agent lens. Daniel Epps identifies three mechanisms that could help reduce agency costs in the secrecy setting, one of which is the use of proxies. Daniel Epps, Note, Mechanisms of Secrecy, 121 Harv. L. Rev. 1556, 1558 (2008). Epps explores the use of proxies only briefly, however, and focuses on government actors who have a direct duty to the public (the FISC and the Executive). His note does not consider the operations of other proxies, such as those treated here as surrogates. Sidney Shapiro and Reina Steinzor use agency theory to evaluate how to hold Congress and the Executive accountable to the public in the face "burgeoning secrecy." Sidney A. Shapiro & Rena I. Steinzor, The People's Agent: Executive Branch Secrecy and Accountability in an Age of Terrorism, 69 Law & Contemp. Probs. 99, 101 (2006). They focus on who should have the power to declassify information, however, not on how other actors can check secret U.S. military and intelligence activities.

[29] Jack Goldsmith, Power and Constraint: The Accountable Presidency After 9/11, at 205–07 (2012).

increased checks and monitoring without sacrificing much secrecy is a desirable development worth sustaining.

This Article makes three contributions. First, it shows descriptively that there are several unsung actors in the government secrecy ecosystem that help guard against the Executive's misuse of secrecy, and that any evaluation of government secrecy that ignores these actors is importantly incomplete. It is well-understood that these types of actors play an important checking function in the public parts of government operations.[30] This Article shows that these actors also serve a checking function behind the veil of secrecy. Second, it analyzes the features of these groups that allow them to provide these checks. It draws attention to their role as necessary actors in the conduct of national security today; their on-the-ground expertise; and their ability to challenge the Executive without disclosing classified information. Third, the Article offers a normative defense of this development, identifying the surrogates' incentives to improve the quality of intelligence, challenge legally questionable executive activities, and demand reasons for secret decisions. Thinking about the existence, role, and possibilities of these unsung secrecy surrogates can sharpen how we approach the challenges of government secrecy; identify where the coincidences of interest lie between these surrogates and the national public; suggest ways to preserve salutary overlaps in interest; and allow us to see where the most pressing gaps in oversight remain.

Part I identifies how the Executive can abuse secrecy, as well as the strengths and weaknesses of our traditional secrecy surrogates. Part II argues that several recent developments in national security threats have positioned technology companies, states and localities, and foreign allies to serve as unsung secrecy surrogates. Part III explores the incentives that these actors have to serve as checks on executive abuses of secrecy and considers how those incentives are aligned with the public law values of legality, accountability, rationality, participation, and, to some extent, transparency. Part IV places these unsung surrogates in the context of a broader "secrecy synopticon." It addresses challenges to the argument that the unsung surrogates can perform robust checking functions and proposes modest ways to enhance their role in the synopticon.

[30] See, e.g., Freeman, supra note 21, at 816–17 (describing how private actors participate publicly in governance through the regulatory process).

I. THE CHALLENGES OF GOVERNMENT SECRECY

Much of the literature on government secrecy bemoans our current system. The familiar tropes are that the Executive overclassifies information, undertakes legally or politically problematic policies in our name without our knowledge, invokes the state secrets privilege to conceal mistakes or abuse, and is miserly about sharing classified or privileged information with Congress. This is a caricature of the way secrecy actually operates within the U.S. system, but there are kernels of truth in each of these precepts. This Part begins by identifying the core reasons why we worry about government secrecy. It then turns to three traditional secrecy surrogates and examines why none of those three actors has been able to mitigate these worries. In doing so, it emphasizes the misalignment of incentives between the Executive and the actors who check it.

A. Why Worry About Government Secrecy?

It is beyond cavil that the executive branch has accreted vast amounts of power to itself in the national security space. One key reason for this is structural: the President controls the officials who collect diplomatic, military, and intelligence information. He also sets the rules for classifying and declassifying that information.[31] As a result of his control over intelligence information and policy execution, the President has the first-mover advantage in national security, leaving Congress and the courts in an inferior position.

In an ideal world, this imbalance would not be problematic. The Executive's acts would always be beyond reproach, and there would be no need to oversee its activities, whether public or secret. As James Madison famously remarked, "If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary."[32] We do not live in an ideal world, of course, and so the public must be concerned about what the Executive does behind closed doors. Past practice has given occasion to

[31] Samuel Rascoff has argued that the President exercises great personal control over covert action and intelligence analysis and relatively less control over intelligence collection (which is left to greater discretion by the intelligence agencies). Samuel J. Rascoff, Presidential Intelligence, 129 Harv. L. Rev. 633, 646 (2016). Even if true, the Executive plays a dominant role in both sets of activities relative to the other branches.

[32] The Federalist No. 51, at 322 (James Madison) (Clinton Rossiter ed., 1961).

worry. To name a few examples, the CIA and FBI famously ran amok in the 1960s and 1970s; President Nixon spied on political adversaries; the Reagan Administration violated the law during the Iran-Contra episode; and the Executive authorized unacceptable interrogation techniques against members of al Qaeda after the September 11 attacks.

The literature identifies a host of ways in which government secrecy can obscure government dysfunction. Executive misuses of secrecy fall into four main categories: concealing poor policy choices; concealing incompetence; concealing legal violations; and avoiding the need to defend executive decisions.[33] There are a host of legitimate reasons why the Executive classifies information; we cannot (and should not seek to) abolish government secrecy entirely. But the possibility and history of misuse makes government secrecy a persistent and thorny challenge.

First, the government may use secrecy to conceal self-enriching policies that the public would condemn if it knew about them.[34] Take President Trump's phone call with Ukrainian President Zelensky. A range of officials who heard the call were troubled by its contents, including the apparent policy decision to withhold military aid to Ukraine unless and until it agreed to investigate Hunter Biden's relationship with a Ukrainian company.[35] At least one of these officials decided to relocate the call transcript to a highly classified system where it would be unlikely to leak. This is an example of a misuse of government secrecy to conceal a self-enriching choice. Another example in this category is the use of secrecy to conceal poor or controversial substantive policy choices. The Obama Administration's decision to secretly obtain the phone records of an Associated Press journalist might serve as an example,[36] as might the bulk telephonic metadata collection program under the USA PATRIOT Act.[37]

[33] See Arthur M. Schlesinger, Jr., The Imperial Presidency 447–49 (2004) ("The real function of the secrecy system in practice is to protect the executive branch from accountability for its incompetence and its venality, its follies, errors and crimes.").

[34] Pozen, supra note 5, at 278 (noting that "secrecy creates greater opportunities for officials to pursue personal or partisan gain").

[35] Peter Baker, In Trump's Ukraine Phone Call, Alarmed Aides Saw Trouble, N.Y. Times (Sept. 26, 2019), https://www.nytimes.com/2019/09/26/us/politics/trump-ukraine-timeline.html [https://perma.cc/NS3V-LYTH].

[36] Kim Zetter, Obama Administration Secretly Obtains Phone Records of AP Journalists, Wired (May 13, 2013, 6:02 PM), https://www.wired.com/2013/05/doj-got-reporter-phone-records/ [https://perma.cc/537N-LD3J].

[37] Press Release, White House, Statement by the President on the Section 215 Bulk Metadata Program (Mar. 27, 2014), https://obamawhitehouse.archives.gov/the-press-

Second, the government may deploy secrecy when it wants to conceal incompetently executed,[38] empirically wrong,[39] or insufficient[40] intelligence, analysis, or operations. Indeed, the current executive order on classification states that executive officials may *not* classify information "in order to conceal violations of law, inefficiency, or administrative error; [or] to prevent embarrassment to a person, organization, or agency . . . ."[41] The fact that the executive order contains this language indicates that this misuse of secrecy has occurred in the past and requires a specific prohibition to address it.[42] Secrecy can also serve as a cause of these problems ex ante, rather than merely a tool for abuse ex post. That is, executive secrecy can prevent obvious incompetence, empirical errors, or shirking from coming to light because fewer actors have the opportunity to press the executive decision maker for explanations and justifications, even if the government is not using secrecy to intentionally hide its missteps. Indeed, utilitarian critics of state secrecy argue that "by inhibiting input, oversight, and criticism within and outside government, secrecy and compartmentalization will often lead to lower-quality policies" and that "debate and dissent may be muted,

office/2014/03/27/statement-president-section-215-bulk-metadata-program [https://perma.cc/4HZC-LY2J].

[38] Doe v. Gonzales, 449 F.3d 415, 422 (2d Cir. 2006) (Cardamone, J., concurring) ("Unending secrecy of actions taken by government officials may also serve as a cover for possible official misconduct and/or incompetence."); Thomas I. Emerson, National Security and Civil Liberties, *in* The First Amendment and National Security 83, 84–85 (1984) ("The secrecy attached to many national security issues allows the government to invoke national security claims in order to cover up embarrassment, incompetence, corruption or outright violation of law.").

[39] Helga Hernes, Foreword, *in* International Intelligence Cooperation and Accountability, at xi (Hans Born, Ian Leigh & Aidan Wills eds., 2011) ("There is an obvious danger that all or part of the information shared with foreign partners could be wrong or inaccurate . . . .").

[40] Johnson, supra note 3, at 61 (quoting intelligence scholar as stating that the major problem facing U.S. intelligence in 2005 was that the "CIA has not been gathering enough quality data"). In agency terms, we might think of this as "shirking."

[41] Exec. Order No. 12,356 § 1.6, 3 C.F.R. 166 (1982). The Obama Administration's policy on the invocation of the state secrets privilege includes comparable language. See Off. of Att'y Gen., Memorandum for Heads of Executive Departments and Agencies & Memorandum for the Heads of Department Components (Sept. 23, 2009), https://www.justice.gov/-archive/opa/documents/state-secret-privileges.pdf [https://perma.cc/2WC2-XYRQ].

[42] See Pallitto & Weaver, supra note 5, at 2–3; Schwarz, supra note 4, at 2 ("[T]oo much is kept secret not to *protect America* but to keep embarrassing or illegal conduct *from Americans*.").

important facts and insights may be overlooked, and preexisting biases may be amplified."[43]

A third problem with government secrecy arises when the Executive uses secrecy to conceal the unlawfulness of its acts.[44] Such actions might include spying on political enemies,[45] engaging in assassination attempts,[46] or transferring individuals to foreign governments to face torture.[47] Even if a program is not patently illegal, the Executive may employ secrecy to preserve programs that are legally tenuous, such as the use of harsh interrogation techniques against al Qaeda members. An Executive that fails to comply with the Constitution or statutes is acting as an unfaithful agent. But if secrecy conceals those abuses, it is impossible for the public as principals to hold it accountable.

There is a fourth reason that the Executive benefits from—and at time abuses—government secrecy. When the Executive can make and execute policies in secret, executive officials need not fight for and defend those programs in the public political process.[48] Particularly where Congress and the President represent different parties or otherwise have an adversarial relationship, the President faces far fewer transaction costs if he can authorize his desired programs and policies in secret and avoid having to defend those choices to Congress or the public.

---

[43] Pozen, supra note 5, at 278.

[44] Pallitto & Weaver, supra note 5, at 7 (discussing how the President's ability to operate in secret prevents Congress and the courts from determining his "constitutional and statutory conformance").

[45] See David S. Law, A Theory of Judicial Power and Judicial Review, 97 Geo. L.J. 723, 745 (2009). As Kiewiet and McCubbins put it, "The essence of the problem is that resources or authority granted to an agent for the purpose of advancing the interests of the principal can be turned against the principal." D. Roderick Kiewiet & Mathew D. McCubbins, The Logic of Delegation: Congressional Parties and the Appropriations Process 26 (1991).

[46] Lynne Duke, Regime Change Assassin? Easier Said Than Done., Wash. Post (Aug. 24, 2005), https://www.washingtonpost.com/archive/lifestyle/2005/08/24/regime-change-assassin-easier-said-than-done/f6494857-8287-4ba9-9028-5880c1f03b0a/ [https://perma.cc/UA2J-RHK9] (describing U.S. attempts to assassinate Castro, Lumumba, and Trujillo).

[47] Comm'n of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Report of the Events Relating to Maher Arar 13–14 (2006), https://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.-ca/eng/AR_English.pdf [https://perma.cc/9H3R-7N9H] (discussing decision by U.S. officials to send Arar to Syria, where he was interrogated and tortured).

[48] Pallitto & Weaver, supra note 5, at 6 ("Where a president may do what is desired in secret, there is no reason to withstand the ordeal of a political battle to achieve the same ends."); Pozen, supra note 5, at 279 (discussing how secrecy provides "insulation from scrutiny").

One way to think about each of these four potential forms of abuse is that they constitute violations of the public law values that we expect the Executive to uphold. Public law values include accountability, rationality, transparency, due process or fairness, competence, and legal compliance.[49] When the Executive acts in secret, it is easier for it to treat those values with less care, and it is more difficult for the public to identify when the Executive is acting in a manner inconsistent with those values. Actions by secrecy surrogates that "check" illegality or flawed execution, force the Executive to justify its decisions to another actor outside the executive branch, or challenge the Executive's classification decisions as excessive therefore can promote public law values.

Each of these potential misuses of government secrecy—acts that are inconsistent with the public law values that we expect the Executive to uphold—engenders public skepticism about secret government activities, at least among some segments of the public.[50] One obvious way to mitigate some of that skepticism is to give other trustworthy actors access to some or all of those executive branch operations, to help minimize the pathologies endemic to government secret keeping. Indeed, core questions that secrecy scholars must ask and answer include: Are there ways to counteract these secrecy-driven problems and to minimize the incentives that the Executive has to abuse secrecy without improperly revealing the secrets themselves? If so, what are those options?

B. The Pathologies of Traditional Surrogates

The traditional answer to these questions has been to turn to the co-equal branches of government. In the wake of the revelations in the Church and Pike reports, Congress and the Executive struck what some call the "grand bargain."[51] As part of that bargain, the Executive was

[49] See, e.g., Freeman, supra note 21, at 818–19; Eichensehr, Public-Private Cybersecurity, supra note 23, at 511 (treating accountability, transparency, and due process as public law values); Laura A. Dickinson, Outsourcing Covert Activities, 5 J. Nat'l Sec. L. & Pol'y 521, 522–26 (2012) (describing transparency, some level of public participation, accountability, and respect for international law as public law values).

[50] Pozen, supra note 5, at 280. Significant segments of the public may be indifferent to abuses of government secrecy. See, e.g., Fenster, supra note 7, at 11 ("[T]oo often, the public appears incapable of acting like the democratic public that transparency assumes must exist. . . . We long for a public that can process and act on information fully and accurately, but it rarely seems to emerge.").

[51] Goldsmith, supra note 29, at 87–93; Jack Goldsmith & Benjamin Wittes, The "Grand Bargain" at Risk: What's at Stake When the President Alleges Politics in Intelligence, Lawfare

allowed to conduct robust intelligence operations, even domestically, but was subject to statutory restrictions on how it did so. The Foreign Intelligence Surveillance Court ("FISC") would oversee the conduct of electronic surveillance, and Congress would conduct extensive oversight behind the veil of secrecy.[52] Thus, the two newly-created intelligence committees ("SSCI" and "HPSCI") and the FISC would be able to check the Executive's secret activities without disclosing the contents of those activities to a wider audience. The intelligence committees and the FISC serve today as secrecy surrogates for the public, in whom we place "transitive trust" that they will help prevent the Executive from abusing secrecy.[53] Secrecy surrogates can engage on at least two levels: they can make procedural judgments about whether the level of secrecy the Executive is employing is appropriate, and they can make substantive judgments about whether Executive's underlying acts are lawful and appropriate or abuses of power.

Congress and the courts both owe loyalty to the public and to public law values, so we might expect them to provide a second-best check on the Executive, behind Madison's angelic Executive. Yet much of the scholarship about government secrecy focuses on the failures of Congress and the courts to act as potent surrogates. One important reason that they have had difficulties—and one reason that the unsung surrogates are distinct from the traditional surrogates—is that the Executive has limited incentives to share information with Congress and the courts, which sometimes lack incentives to demand it.[54] This Section first examines the

(Apr. 4, 2017, 2:39 PM), https://www.lawfareblog.com/grand-bargain-risk-whats-stake-when-president-alleges-politics-intelligence [https://perma.cc/E3U6-X8XK].

[52] Goldsmith & Wittes, supra note 51 (describing the "grand bargain").

[53] Deeks, Reason-Giving, supra note 9, at 645 (articulating the concept of "transitive trust"); see also Michael E. DeVine, Cong. Rsch. Serv., R45196, Covert Action and Clandestine Activities of the Intelligence Community: Framework for Congressional Oversight in Brief (2019) ("Congressional oversight of intelligence, therefore, is unlike its oversight of more transparent government activities with a broad public following. In the case of the Intelligence Community, congressional oversight is one of the few means by which the public can have confidence that intelligence activities are being conducted effectively, legally, and in line with American values.").

[54] Although this Article does not focus on actors who can check government secrecy from within the Executive, some executive actors play this role (such as Inspectors General, General Counsels, and policymakers who are in touch with outside constituencies). Further, the Executive has created procedural tools to help it monitor abuses of secrecy, such as internal rules to prevent classification of information or the invocation of the state secrets privilege in court to conceal embarrassment.

challenges Congress faces in serving as a secrecy surrogate, then turns to the courts, whistleblowers, and leakers.

1. Congressional Committees

Congress possesses some compelling incentives to serve as a faithful surrogate. First, members of Congress take an oath or affirmation to support the Constitution.[55] That oath includes a commitment to the structural aspects of the Constitution, including separation of powers and checks and balances. Although increasingly rare, some members of Congress retain a tangible commitment to the institution of Congress itself, not just to their constituents, and so work to preserve the roles and entitlements of Congress as a body. This includes a commitment to providing genuine oversight over the Executive.[56] Second, politics can stimulate members of Congress to carefully oversee acts of a President of a different political party.[57] Third, members of Congress are susceptible to embarrassment ex post if they ignore or overlook executive abuses that happen on their watch. Intelligence overseers were embarrassed, for instance, in the wake of the Iran-Contra affair.[58] Finally, at some level members of Congress are the best possible surrogates for the public, because they must stand for elections and are thus closely attuned to the sentiments of their constituents.[59]

Nevertheless, as in all principal-agent relationships, Congress serves as an imperfect agent for the public. First, members of the intelligence committees lack strong incentives to provide effective oversight because they are poorly rewarded for doing so.[60] Amy Zegart notes that it is

[55] U.S. Const. art. VI, cl. 3.

[56] Press Release, Sen. Dianne Feinstein, Statement on Intel Committee's CIA Detention, Interrogation Report (Mar. 11, 2014), https://www.feinstein.senate.gov/public/index.cfm/-2014/3/feinstein-statement-on-intelligence-committee-s-cia-detention-interrogation-report [https://perma.cc/R9S2-Q54Z].

[57] Daryl J. Levinson & Richard H. Pildes, Separation of Parties, Not Powers, 119 Harv. L. Rev. 2311, 2327 (2006).

[58] Johnson, supra note 3, at 64.

[59] There is some question about the extent to which the general population cares about excessive government secrecy. Shapiro & Steinzor, supra note 28, at 100 ("[T]he public seems generally apathetic regarding [executive decisions to deny Freedom of Information Act requests]."); Neal Kumar Katyal, Stochastic Constraint, 126 Harv. L. Rev. 990, 1000 (2013) (reviewing Jack Goldsmith, Power and Constraint: The Accountable Presidency After 9/11 (2012)) (describing the "popular willingness to err on the side of national security").

[60] See Amy B. Zegart, Future Challenges: The Roots of Weak Congressional Intelligence Oversight, Hoover Inst., June 14, 2010, at 4, https://www.hoover.org/sites/default/files/-

difficult for intelligence committee members to receive credit from their constituents for the intelligence oversight they conduct.[61] Further, it is hard for those members to exercise strong control over the intelligence community via appropriations because most of the intelligence budget is buried within the Defense Department's budget, which deprives the committee authorizers of leverage.[62] Additionally, members of Congress sometimes prefer not to be fully briefed about potentially controversial secret programs, to avoid being tainted electorally if the programs go badly.[63] Members of Congress sometimes become co-opted by the executive branch because they over-identify with the intelligence community[64] or choose to be unduly deferential because they believe that the intelligence community has deeper experience than they do.[65] Finally, members of Congress might choose not to challenge the Executive in certain contexts for fear of losing access to intelligence that the Executive has the discretion but not the obligation to share, or because they wish to protect the President politically. All of these incentives render congressional committees less than fully effective overseers.

Second, as a practical matter, congressional committees may lack sufficient capacity and expertise to conduct robust oversight. The committees are understaffed: HPSCI has about two dozen staffers to oversee an intelligence community of 107,000 people (as of 2017).[66] The members themselves often have limited expertise in intelligence before they join the committees, and the classified nature of the work makes it more complicated and time-consuming for those members to read

research/docs/future-challenges-zegart.pdf [https://perma.cc/QQW6-V9G8] (stating that her "research suggests that Congress has struggled with intelligence oversight for a long time").

[61] Id. at 7; Johnson, supra note 3, at 68–69 (discussing limited commitment of intelligence overseers to their jobs).

[62] Zegart, supra note 60, at 13; Michael E. DeVine, Cong. Rsch. Serv., R44381, Intelligence Community Spending: Trends and Issues 11 (2019).

[63] House Speaker Nancy Pelosi denied knowing about waterboarding, for instance. Marc A. Thiessen, Ex-CIA Counterterror Chief Says Pelosi "Reinventing the Truth" About Waterboarding, Wash. Post (Apr. 30, 2012), https://www.washingtonpost.com/-opinions/ex-cia-counterterror-chief-pelosi-lied-about-waterboarding/2012/04/30/gIQAQFG-trT_story.html [https://perma.cc/8N4K-HZEP].

[64] Johnson, supra note 3, at 72; Tim Johnson & Ben Wieder, Intelligence Committees Lean on Ex-Spies To Oversee Spy Agencies, McClatchy (Sept. 5, 2017, 4:40 PM), https://www.mcclatchydc.com/news/nation-world/national/article170815177.html [https://perma.cc/G2RV-DLNR] (discussing "capture" of intelligence committees by intelligence agencies).

[65] Johnson, supra note 3, at 72.

[66] Johnson & Wieder, supra note 64.

background documents and attend briefings. The committees' rotation rules, which were crafted to avoid co-optation, end up limiting the amount of expertise that members are able to develop.[67] Finally, it is far from clear that members or staffers have the technological sophistication necessary to provide deep oversight over programs involving complicated electronic surveillance, cyber, or artificial intelligence technologies.[68]

Third, the Executive has the power to deny Congress access to certain intelligence programs, even when Congress demands that it be kept fully informed. The fact that the Executive exclusively collects, classifies, and analyzes intelligence renders this a structural problem that is difficult for Congress to remedy.[69] The Executive by statute is required to keep Congress "fully and currently informed of the intelligence activities of the United States,"[70] including covert actions, but Congress has difficulty getting access to information about certain programs.[71] For instance, it took Congress almost a year to obtain access to U.S. Cyber Command's rules regulating offensive cyber operations.[72] The Executive also is cautious about sharing intelligence with Congress when the information comes from foreign partners because it views leaks of partner intelligence

[67] Zegart, supra note 60, at 8–10; Johnson, supra note 3, at 72.

[68] Jenna McLaughlin, Congress May Lack Technical Expertise to Properly Investigate Russian Hacking, Intercept (Feb. 28, 2017, 10:38 AM), https://theintercept.com/-2017/02/28/congress-may-lack-technical-expertise-to-properly-investigate-russian-hacking/ [https://perma.cc/Y7YM-LT9V] (noting that the bulk of intelligence committees' staff are "lawyers, policy wonks, and budget experts" rather than experts in "coding, information security, and attribution"); Zach Graves & Daniel Schuman, The Decline of Congressional Expertise Explained in 10 Charts, Techdirt (Oct. 18, 2018, 11:55 AM), https://www.techdirt.com/articles/20181018/10204640869/decline-congressional-expertise-explained-10-charts.shtml [https://perma.cc/QWD4-XMBU].

[69] See Pozen, supra note 5, at 318–19 (noting that "some amount of publicity is a necessary precondition for information-access disputes to arise in the first place" and that "Congress and the public will always be the 'losers' of access disputes that never materialize").

[70] 50 U.S.C. §§ 3091–93 (2012).

[71] Johnson, supra note 3, at 70 (noting that "Congress's Joint Committee complained in 2002 about stonewalling by the second Bush Administration"); Sudha Setty, National Security Secrecy 39–41 (2017); Michael E. DeVine, Cong. Rsch. Serv., R45720, United States Foreign Intelligence Relationships: Background, Policy and Legal Authorities, Risks, Benefits 8 (2019) (noting that Congress has difficulty overseeing classified intelligence sharing agreements).

[72] Joseph Marks & Tonya Riley, The Cybersecurity 202: Congress Peels Back Secrecy To Review Trump Hacking Policy, Wash. Post (Dec. 18, 2019, 7:54 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/12/-18/the-cybersecurity-202-congress-peels-back-secrecy-to-review-trump-hacking-policy/5d-f9136b602ff125ce5b5c45/ [https://perma.cc/LAL7-PDDG].

as particularly harmful.[73] More generally, the Executive seeks to preserve its institutional authorities from encroachment, even if in a particular instance it might not be costly to share information about a program or policy.[74]

In sum, while the Executive provides the intelligence committees with a significant number of briefings and reports about the intelligence community's activities, Congress's ability and willingness to conduct effective oversight is hindered by its sometimes perverse motivations and its limited expertise, especially in technical areas, as well as the Executive's persistent incentives to withhold certain information from Congress.

2. Federal Courts

Like Congress, courts that encounter cases implicating secret government operations have some incentives to serve as effective surrogates for the public in checking government illegality. First, judges take an oath to uphold the law and must identify illegality in those cases over which they have jurisdiction. Second, judges seek to preserve their reputation among their peers and the public.[75] For instance, in a rendition case involving state secrets, the Ninth Circuit went to great lengths to try to persuade the public of its credibility as a secrecy surrogate by discussing the care with which it reviewed the government's (classified) claims.[76] The court noted:

> We . . . acknowledge that this case presents a painful conflict between human rights and national security. As judges, we have tried our best to evaluate the competing claims of plaintiffs and the government and resolve that conflict according to the principles governing the state secrets doctrine set forth by the United States Supreme Court.[77]

[73] Hernes, supra note 39, at xi ("[N]ational oversight bodies are usually either obliged to show restraint in asking for access to such material, or they are totally cut off from it.").

[74] Pallitto & Weaver, supra note 5, at 3 (noting executive interest in "maintain[ing] presidential prerogative against congressional inquiries and judicial orders").

[75] Deeks, Reason-Giving, supra note 9, at 622–23.

[76] Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1092–93 (9th Cir. 2010) (en banc).

[77] Id. at 1093; see also N.Y. Times Co. v. U.S. Dep't of Just., 915 F. Supp. 2d 508, 515 (S.D.N.Y. 2013) (in which the judge bemoaned the "Alice-in-Wonderland"-like quality of the case and her inability to force the government to disclose a Justice Department opinion).

Third, unlike members of Congress, judges with life tenure can afford to be less susceptible to political pressures. In short, the courts possess baseline incentives to check secret executive activities in egregious cases.

The courts face several hurdles to serving as robust secrecy surrogates, however. First, they necessarily are reactive: they can only hear cases that others bring. This means that they review only a small subset of secret government activities. Other than the FISC, which engages deeply with executive requests to conduct classified foreign intelligence surveillance, federal courts only sporadically confront cases that implicate government secrecy: in the past decade they have heard several cases involving renditions and surveillance in which the government invoked the state secrets privilege;[78] about a dozen litigated uses of the Classified Information Procedures Act;[79] an occasional use of force case involving military operations;[80] and some national security-focused Freedom of Information Act litigation.[81]

Second, the Executive has traditionally proven very reluctant to make classified information available to courts (other than the FISC). The government often expresses concern about leaks[82] and argues for extensive judicial deference to its decisions.[83] Third, and relatedly, for separation of powers and competence reasons, courts traditionally defer to executive assertions about national security equities, classification questions, and factual issues linked to intelligence or military decisions.[84] Fourth, like Congress, courts perceive that national security decisions have high stakes and worry about reaching decisions that might result in national security harms.[85] For all of these reasons, the courts often rely on a range of non-justiciability doctrines, including the political question doctrine and the state secrets privilege, to avoid wading deeply into the

[78] See, e.g., *Mohamed*, 614 F.3d 1070.

[79] See, e.g., United States. v. El-Mezain, 664 F.3d 467 (5th Cir. 2011).

[80] See, e.g., Hedges v. Obama, 724 F.3d 170 (2d Cir. 2013).

[81] See, e.g., ACLU v. U.S. Dep't of Def., 628 F.3d 612 (D.C. Cir. 2011).

[82] See, e.g., United States v. U.S. Dist. Ct. for the E. Dist. of Mich., 407 U.S. 297, 319 (1972).

[83] See Robert M. Chesney, National Security Fact Deference, 95 Va. L. Rev. 1361, 1362 (2009) (noting that the executive branch often argues that judges should defer to its factual judgments in national security cases).

[84] See, e.g., Sagar, supra note 7, at 55 ("Can judges, far removed from the cut and thrust of diplomacy and international intrigue, really challenge the president's contentions as to what information should not be made public?").

[85] Chesney, supra note 83, at 1428 (discussing judicial concerns about institutional self-preservation in national security cases).

Executive's intelligence or military activities.[86] While the FISC serves as a credible surrogate in the electronic surveillance space, federal courts generally face a range of challenges to serving as robust secrecy surrogates.[87]

3. Whistleblowers, Leakers, and Journalists

Whistleblowers, leakers, and journalists are bolder surrogates than courts but lack their constitutional imprimatur.[88] Nevertheless, much of the scholarship on government secrecy portrays whistleblowers and leakers as an important supplement to the constitutional checks on the Executive from the other branches. For the most part, this literature identifies the positive potential of statutory whistleblowing regimes but views the current system as ineffectual as a practical matter.[89] It treats leakers as an unfortunate but critical aspect of our secrecy ecosystem.[90]

Whistleblowers in national security agencies have the potential to serve as important secrecy surrogates: they have access to classified information, can identify problematic executive activity, and can report it in a way that does not expose classified information to the public. In

[86] See, e.g., Al-Aulaqi v. Obama, 727 F. Supp. 2d 1, 45 (D.D.C. 2010) ("An examination of the specific areas in which courts have invoked the political question doctrine reveals that national security, military matters and foreign relations are 'quintessential sources of political questions.'" (quoting El-Shifa Pharm. Indus. Co. v. United States, 607 F.3d 836, 841 (D.C. Cir. 2010))); Laura K. Donohue, The Shadow of State Secrets, 159 U. Pa. L. Rev. 77, 85–86 (2010) (noting that there have been over four hundred state secrets cases since 1953).

[87] Even here, the FISC has its limits as a surrogate because it usually only hears the government's arguments. Under the USA FREEDOM Act, the FISC can now appoint amici to help it address challenging legal questions by offering a perspective that may differ from the government's. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 279.

[88] I use "whistleblower" to mean someone who attempts to reveal evidence of executive waste, fraud, abuse, or illegality by following statutorily-created channels. See, e.g., Whistleblower Protection Act of 1989, Pub. L. No. 101-12, 103 Stat. 16 (codified as amended in scattered sections of 5 U.S.C.); Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112-199, 126 Stat. 1465; Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, §§ 701–02, 112 Stat. 2396, 2413–17 (codified as amended at 5 U.S.C. § 8H, 50 U.S.C. § 3033(k)(5), and 50 U.S.C. § 3517); Whistleblower Protection for Contractor and Grantee Employees, Pub. L. No. 114-261, 130 Stat. 1362 (2016). I use "leaker" to mean someone who reveals classified information to a journalist with the expectation of anonymity. See Sagar, supra note 7, at 202–03.

[89] David E. Pozen, The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information, 127 Harv. L. Rev. 512, 527 (2013).

[90] See, e.g., Sagar, supra note 7, at 204 ("That we must rely on a regulatory weapon [i.e., leaking] that has the tendency to backfire at least as often as it finds its target—*this* is the dilemma that state secrecy creates for democracy.").

general, whistleblower statutes establish procedures by which whistleblowers report their concerns to their agency's inspector general ("IG"), who can report the information to the appropriate congressional committee if the IG finds it credible.[91] The statutes protect whistleblowers against retaliation if they follow this process. However, the process rarely works as intended: the statutes are not user friendly and do not prevent agencies from revoking whistleblowers' security clearances, which provides a disincentive for whistleblowers to come forward.[92] Whistleblowers thus play only a minor surrogacy role in the national security space.

Unlike whistleblowers, national security leakers often act anonymously and disclose classified information to journalists who then publish it. Leaking classified information poses several obvious problems. First, and most obviously, it is generally illegal.[93] Second, the information that leakers reveal can adversely impact national security or can be misleading because the leaker only reveals a small piece of the overall landscape. Third, those engaged in leaks may be motivated by self-aggrandizement or revenge; at the very least, they arrogate authority to themselves to make policy decisions that they lack the legal right to make. Fourth, as Neal Katyal notes, "leaking as a check suffers from the same problem as the judicial check—it is far too haphazard a practice around which to build a constitutional system."[94]

Leaking admittedly provides some benefits in the secrecy ecosystem. Scholars such as Bruce Ackerman view leaking in a positive light, arguing that leakers are "patriotic" and that their disclosures promote our national security by "preserving our constitutional integrity."[95] Further, the threat of leaks may have a positive impact on executive behavior ex ante if the Executive perceives that decisions it makes in secret may become public

[91] See, e.g., Intelligence Community Whistleblower Protection Act §§ 701–02; see also Michael E. DeVine, Cong. Rsch. Serv., R45345, Intelligence Community Whistleblower Protections 2 (2019) (discussing intelligence community whistleblower protections).

[92] See Pozen, supra note 89, at 527 (noting that in the national security context whistleblowers "play a marginal role").

[93] See id. at 522–24 (listing range of criminal statutes that apply or might apply to leaking).

[94] Katyal, supra note 59, at 1003.

[95] Bruce Ackerman, Protect, Don't Prosecute, Patriotic Leakers, N.Y. Times (June 12, 2012), https://www.nytimes.com/2012/06/13/opinion/dont-prosecute-leakers-who-defend-our-constitution.html [https://perma.cc/D8ZC-3PDN].

in the short term.[96] Finally, some leakers reveal very problematic executive acts that the public would want to see halted and condemned.

Even those scholars who recognize that leaks can impose serious costs often conclude that it is difficult to conceive of a system superior to one that periodically tolerates leaks while prosecuting some leakers.[97] David Pozen, for instance, identifies the commonly held and somewhat paradoxical view that "leaking 'is a problem of major proportions' and that 'our particular form of government wouldn't work without it.'"[98] This tolerance for some level of leaks reflects a frustration with the weaknesses of our congressional and judicial surrogates.

Journalists are an important part of the secrecy ecosystem as well: through journalists, the leaks' contents find their way into the public conversation. Like leakers, journalists lack constitutional duties to the public and have a range of incentives to reveal classified information. Journalists often see themselves as acting in the public interest and argue that revealing secret government abuses of authority advances the public's interest in an accountable government.[99] Responsible journalists try to balance U.S. national security equities against the public interest in understanding what the government is doing,[100] though they sometimes strike that balance incorrectly.[101] Journalists also seek to sell newspapers,

[96] Deeks, Reason-Giving, supra note 9, at 649.

[97] Goldsmith, supra note 29, at 218 ("And so we have a system in which the executive branch, in the secret aspects of its wars and intelligence operations, sometimes makes mistakes that can harm national security, and in which the press and others seeking to hold the executive branch accountable sometimes publish information that can harm national security. There are costs and benefits to national security from both secrecy and disclosure . . . .").

[98] Pozen, supra note 89, at 514 (citations omitted).

[99] See RonNell Andersen Jones, Litigation, Legislation, and Democracy in a Post-Newspaper America, 68 Wash. & Lee L. Rev. 557, 591 (2011) (noting that the media "have routinely acted as proxy for the larger public, putting the legislative tools to use after fighting for their enactment").

[100] Barton Gellman, Secrecy, Security and Self-Government: An Argument for Unauthorized Disclosures, Century Found. (Sept. 3, 2013), https://tcf.org/content/-commentary/secrecy-security-and-self-government-an-argument-for-unauthorized-disclosures/ [https://perma.cc/N5WK-QUKZ] ("The Washington Post and its peers routinely consult responsible agencies before publishing anything classified. . . . We often ask for explanation of the stakes. . . . We can identify more and less harmful forms of secrecy, better and worse reasons to withhold information from 'we the people,' and factors that heighten and diminish the case for disclosure. . . . Sometimes strong security interests collide with weak public interests in disclosure. . . . We seldom if ever agree to withhold information that exposes a government lie, even a well-intended one.").

[101] Goldsmith, supra note 29, at 213–18 (providing examples of media disclosures of leaked information that had significant negative consequences for intelligence gathering).

however, and publishing secrets is a surefire way to achieve that.[102] Journalists thus serve as another example of secrecy surrogates who—like leakers—often reveal classified information in situations in which the public might not agree with the fact of the disclosures.

In short, while leakers and journalists can sometimes reveal problematic, inept, or illegal programs that the public ultimately condemns, their actions can have a significant adverse impact on national security. It is problematic, then, that many scholars and practitioners have the intuition that a system that uses leaks as a backstop is the best we can do. In David Cole's words, "leakers are a terrible answer to the problem, but they're the only answer we have to the problem."[103] The next Part challenges that conclusion, arguing that there are several other categories of secrecy surrogates whose ability to check the Executive's misuse of secrecy complements that of the surrogates discussed in this Part, and who can do so without compromising national security.

II. SECURITY THREATS AND UNSUNG SECRECY SURROGATES

If our traditional secrecy surrogates have produced an ecosystem in which certain actors unpredictably reveal classified information, while other actors are unwilling or unable to systematically guard against executive illegality, incompetence, or poor policy choices, is there any reason to be optimistic that other actors could improve executive behavior in the secrecy space? Congress has the purse, after all; the courts have judicial power; and leakers can upend secret U.S. government programs in a single afternoon. As Part I suggests, however, Congress and the courts have a variety of disincentives to patrol aggressively, while leakers serve as erratic, problematic checks at best. Further, the Executive has incentives to engage with these surrogates at the most minimal level that

[102] See Note, Media Incentives and National Security Secrets, 122 Harv. L. Rev. 2228 (2009) (exploring how the media makes decisions about publishing national security secrets).

[103] Alex Abdo, David Cole, George Ellard, Kenneth Wainstein & Stephen I. Vladeck, A New Paradigm of Leaking, 8 J. Nat'l Sec. L. & Pol'y 5, 31 (2015); see also Gellman, supra note 100 ("It turns out that I am making an argument for something like the status quo. In practice today, the flow of information is regulated by a process of struggle. The government tries to keep its secrets, and people like me try to find them out. Intermediaries, with a variety of motives, perform the arbitrage. No one effectively exerts coercive authority at the boundary. And that's a good thing."); Sagar, supra note 7, at 203 (arguing that sporadic leaks are the best realistic option for our system); Pozen, supra note 89 (describing how leaks are an integral mechanism by which the government discloses information).

it can get away with, because these actors generally do not directly facilitate the Executive's intelligence or military operations.[104]

This Part argues that we have failed to appreciate another set of secrecy surrogates who can reduce abuses of government secrecy—and already have done so in some cases. Today, key U.S. national security threats include hostile cyber operations, threats to our electoral systems, and terrorism. The federal government is not, however, the exclusive target of these threats, nor can it respond to those threats on its own. Instead, the targets themselves—including technology companies, states and localities, and U.S. allies—must play a part in responding. This means that there is a range of actors with whom the executive branch must work cooperatively to address the threats. The Executive has chosen to—and presumably feels that it must—share classified information about threats and operations with these players. These actors have the opportunity to assess the quality and quantity of the information and, in some cases, the legality of the underlying executive activities. They also serve as an important and diverse audience for the Executive, one that forces it to offer persuasive reasons for its actions and thus potentially improve its decision making ex ante.[105] The Director of the U.S. National Counterintelligence and Security Center recently acknowledged as much, stating, "Industry is going to have to make the government more accountable and hold us to what we want to do."[106]

This Part first describes the new threat landscape. It then lays out the ways in which technology companies, states and localities, and foreign allies are engaging with the Executive to address these threats.

A. Contemporary Threats to National Security

The United States is facing at least two new types of critical security threats: cyber threats and threats to its electoral systems. It also continues

[104] The Executive admittedly needs the FISC in a limited legal sense, because the Executive cannot undertake certain kinds of electronic surveillance without the FISC's authorization. Likewise, the Executive needs Congress's appropriations, and so must share some minimum amount of information to ensure the appropriations are forthcoming. The Executive does not need other internal actors such as the PCLOB or PIAB, except to the extent that the Executive can use these groups to bolster its own legitimacy.

[105] See Deeks, Reason-Giving, supra note 9.

[106] Mariam Baksh, ODNI Plans To Share More About Cyber Threats Under New Counterintelligence Strategy, Nextgov (Feb. 4, 2020) (internal quotation marks omitted), https://www.nextgov.com/cybersecurity/2020/02/odni-plans-share-more-about-cyber-threats-under-new-counterintelligence-strategy/162881/ [https://perma.cc/H8SA-FJ5Y].

to face the kinds of terrorist threats that became highly salient after September 11, 2001.[107] Both states and non-state actors possess the tools to engage in all three types of activities.[108] Traditionally, the primary national security threats to the United States came from state adversaries, which sought to obtain intelligence about and obstruct U.S. military and intelligence operations. Today, however, foreign states and non-state actors target not only the federal government but also state and local governments, private companies, and individuals. Although the federal government plays a role in defending all of these targets, each target also plays a role in defending itself. Additionally, technology and cybersecurity companies such as Microsoft, Google, and Mandiant provide defensive assistance to these targets.

The shift away from the federal government as the primary target and sole responder to these threats has been a seismic one for national security. As the General Counsel of the National Security Agency recently wrote:

> [One] implication of the digital revolution is that the balance between government and the private sector will be altered in a profound way. That in turn is the inescapable product of three factors: cyber-vulnerability affecting every element of the private sector (no longer are targets arguably limited to military assets), the general flood of data unleashed by the digital revolution that will be created in the hands of private enterprise and a response to a rising China whose strategic technology goals pose a unique threat that directly implicates the private sector.[109]

In short, a range of actors are producing new security threats aimed at new targets, and the Executive has turned to new (or under-appreciated) players to help defend those targets. One complicating feature of this

[107] See Coats, supra note 12, at 5–13 (listing cyber, online influence operations and election interference, weapons of mass destruction and proliferation, and terrorism as major global threats); see also William Ford, The Senate Examines Threats to the Homeland, Lawfare (Nov. 7, 2019, 5:47 PM) (emphasizing threats posed by domestic terrorism, Chinese cyber operations, and new technologies, including ransomware).

[108] Nat'l Counterintelligence & Sec. Ctr., Foreign Threats to U.S. Elections: Election Security Information Needs, https://www.dni.gov/files/ODNI/documents/DNI_NCSC_Elections_Brochure_Final.pdf [https://perma.cc/323Z-39YH] (last visited Oct. 12, 2020) (describing election interference by foreign states and non-state actors).

[109] Glenn S. Gerstell, I Work for N.S.A. We Cannot Afford To Lose the Digital Revolution., N.Y. Times (Sept. 10, 2019), https://www.nytimes.com/2019/09/10/opinion/nsa-privacy.html [https://perma.cc/2W5N-T4G7].

development is that much of the federal government's intelligence about these threats is classified, which means that the government increasingly must share classified information and plans to defeat the threats with new players.

1. Hostile Cyber Operations and Supply Chain Manipulation

It is difficult to overstate the size of the threat that foreign cyber operations pose to U.S. national security.[110] The growth of the Internet initiated this shift as federal, state, and local governments, companies, and individuals came to rely on it for a huge range of purposes, creating new targets for foreign adversaries. The Intelligence Community's 2019 Worldwide Threat Assessment identifies hostile cyber operations as a global threat and notes:

> China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure. . . . As we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information.[111]

The corruption of supply chains is a related technological threat. At the federal level, foreign adversaries try to corrupt U.S. military and intelligence supply chains by introducing counterfeit or malicious items into them, creating vulnerabilities in the government's weapons systems or intelligence collection tools.[112] These adversaries also try to penetrate the supply chains of U.S. companies, states, and localities with the goal of stealing information that passes through or is collected by these U.S. actors.[113]

---

[110] For general background on cyber threats, see, e.g., John P. Carlin & Garrett M. Graff, Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat (2018); Shane Harris, @War: The Rise of the Military-Internet Complex (2014).

[111] Coats, supra note 12, at 5.

[112] Off. of the Dir. of Nat'l Sec., ICS 731-02, Supply Chain Threat Assessments (2016), https://www.dni.gov/files/NCSC/documents/supplychain/ICS%20731-02%20Supply%20Chain%20Threat%20Assessments%20(U).pdf [https://perma.cc/LB9Q-MTMJ]; Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, 132 Stat. 5173, tit. II (2018) (creating the Federal Acquisition Security Council to assess supply chain risk and protect U.S. acquisition of information and communication technologies).

[113] See Exec. Order No. 13,873, 84 Fed. Reg. 22,689 (May 15, 2019).

When adversarial foreign states or non-state actors use cyber tools or supply chain vulnerabilities to conduct espionage or attack the systems of the federal government alone, the federal government will not necessarily need to share information with other actors about those operations. It can keep its detection, analysis, attribution, and response to itself because it has control over and extensive knowledge about the systems affected by the threats, and the capacity to analyze the sources of the threats, establish defenses, and assess how best to respond.[114]

However, U.S. adversaries do not direct their cyber operations exclusively against the federal government and its systems. The adversaries are also targeting private companies, as North Korea did when it wiped out seventy percent of the computer capabilities of Sony Pictures,[115] and as Iran has done with U.S. telecommunications companies and banks.[116] The U.S. intelligence community has assessed that China "will authorize cyber espionage against key US technology sectors when doing so addresses a significant national security or economic goal not achievable through other means."[117] Foreign states have also targeted critical infrastructure: Iran conducted a cyber attack on the controls of a New York dam in 2016, for example, and Chinese state-sponsored hackers directed a spear-phishing campaign against employees at three major U.S. utility companies.[118]

[114] The government also may choose to disclose such operations, as it did with the Chinese theft of millions of records from the Office of Personnel Management. Brendan I. Koerner, Inside the Cyberattack That Shocked the US Government, Wired (Oct. 23, 2016, 5:00 PM), https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ [https://perma.cc/TCP4-EYHP].

[115] David E. Sanger & Katie Benner, U.S. Accuses North Korea of Plot To Hurt Economy as Spy Is Charged in Sony Hack, N.Y. Times (Sept. 6, 2018), https://www.nytimes.com/2018/09/06/us/politics/north-korea-sony-hack-wannacry-indictment.html [https://perma.cc/V3T2-E7GE].

[116] Nicole Perlroth & Katie Benner, Iranians Accused in Cyberattacks, Including One That Hobbled Atlanta, N.Y. Times (Nov. 28, 2018), https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html (telecommunications companies) [https://perma.cc/3RTX-CSHZ]; David E. Sanger, U.S. Indicts 7 Iranians in Cyberattack on Banks and a Dam, N.Y. Times (Mar. 24, 2016), https://www.nytimes.com/2016/03/25/world/middleeast/us-indicts-iranians-in-cyberattacks-on-banks-and-a-dam.html [https://perma.cc/3K2X-964H] (banks).

[117] Coats, supra note 12, at 5.

[118] Sanger, supra note 116 (Iran); Ctr. for Strategic & Int'l Stud., Significant Cyber Incidents Since 2006, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents [https://perma.cc/3FSE-U2ES] (China).

Foreign governments are even conducting cyber operations against U.S. states: in 2019, a "state-sponsored hacking campaign knocked offline more than 2,000 websites across Georgia, including government and court websites."[119] States and cities have been the targets of a number of high-profile ransomware operations, too, some with links to foreign states. Ransomware took down the City of Baltimore's "voice mail, email, a parking fines database, and a system used to pay water bills, property taxes and vehicle citations."[120] The hackers may have been from Russia or Eastern Europe.[121] In 2018, the City of Atlanta also faced a destabilizing ransomware attack, possibly by Iranian hackers.[122] These incidents are not unique: since 2013 there have been at least 169 ransomware attacks on state and local governments.[123]

Like cyber threats, supply chain threats are not exclusively the problem of the federal government. In 2018, the United States created the Cybersecurity and Infrastructure Security Agency ("CISA"), which helps safeguard U.S. critical infrastructure from cyber and physical threats and vulnerabilities.[124] Much of the infrastructure that may be adversely affected by corrupted supply chains is owned by states, localities, or private companies, so CISA works with those actors to minimize supply chain vulnerabilities.[125] Further, because the United States shares intelligence with foreign allies using telecommunications and related infrastructure, the United States sees infrastructure supply chain threats

[119] Ctr. for Strategic & Int'l Stud., supra note 118.

[120] Niraj Chokshi, Hackers Are Holding Baltimore Hostage: How They Struck and What's Next, N.Y. Times (May 22, 2019), https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html [https://perma.cc/TKN6-FNQ8].

[121] Id.; see also Luke Broadwater, Baltimore Transfers $6 Million To Pay for Ransomware Attack; City Considers Insurance Against Hacks, Balt. Sun (Aug. 28, 2019), https://www.baltimoresun.com/politics/bs-md-ci-ransomware-expenses-20190828-njgznd7-dsfaxbbaglnvnbkgjhe-story.html [https://perma.cc/Q4EA-W5WY] (estimating that recovering from the hack would cost Baltimore $18 million).

[122] Chokshi, supra note 120; Perlroth & Benner, supra note 116 (noting that hackers had collected over six million dollars in ransom payments from various targets, including the City of Newark, Colorado's Department of Transportation, and hospitals and health care groups in several states).

[123] Chokshi, supra note 120.

[124] Coats, supra note 12, at 5 ("We are also concerned about the potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies."); CISA, About CISA (Aug. 23, 2020), https://www.cisa.gov/about-cisa [https://perma.cc/YT8G-E98H].

[125] CISA, Strategic Intent (Aug. 2019), https://www.cisa.gov/sites/default/files/-publications/cisa_strategic_intent_s508c.pdf [https://perma.cc/Z7R3-GVAU] (noting that CISA works with partners across government and industry).

to its allies as a threat to itself. The case of Huawei serves as an example: the United States has actively urged a range of countries, including the United Kingdom, Germany, Poland, Australia, and Japan, not to purchase Huawei equipment for use in their 5G networks because the United States believes that Huawei will share with China the metadata or content that crosses those networks.[126]

In short, cyber and supply chain threats pose a robust challenge not only to the federal government but also to states and localities, private companies (including companies responsible for critical infrastructure), and foreign allies. As a result, these non-federal actors have assumed a new role in U.S. national security, and the federal government must treat them as partners in protecting the country.[127] As discussed in Section II.B, at least some aspects of this cooperation take place in a classified setting.

2. Election Interference

Before 2016, few contemplated that elections would be a national security battlefield.[128] As the Mueller Report recounted, however, the Russian government used the 2016 elections to advance its foreign policy goals by creating divisions among the American public, casting doubt on the integrity of the U.S. democratic process, and promoting the election to the White House of its preferred candidate.[129] Reflecting the

[126] Julian E. Barnes & Adam Satariano, U.S. Campaign To Ban Huawei Overseas Stumbles as Allies Resist, N.Y. Times (Mar. 17, 2019), https://www.nytimes.com/2019/-03/17/us/politics/huawei-ban.html [https://perma.cc/JT9N-2EAS].

[127] See Baksh, supra note 106 (discussing ODNI's cyber strategy, which takes "a 'whole of society' approach that hopes to encourage greater private-sector participation in protecting the country from cyber threats").

[128] As Chris Painter, a former cyber official in the U.S. State Department, noted, "We'd never expected that the Russians would do this, attacking our vital infrastructure and undermining our democracy." Huib Modderkolk, Dutch Agencies Provide Crucial Intel About Russia's Interference in U.S. Elections, De Volkskrant (Jan. 25, 2018, 9:00 PM), https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/ [https://perma.cc/6HAR-83CQ]; U.S. Dep't of State, Bureau of Pub. Affairs, Christopher Painter, https://2009-2017.state.gov/r/pa/ei/biog/-161848.htm [https://perma.cc/CZ2A-YRSK] (last visited Sept. 28, 2020).

[129] Robert S. Mueller III, 1 Report on the Investigation into Russian Interference in the 2016 Presidential Election 4 (2019), https://www.justice.gov/storage/report.pdf [https://perma.cc/-U664-JGDD]; see also Nat'l Counterintelligence & Sec. Ctr., supra note 108 ("Foreign intelligence entities likely view U.S. elections as an opportunity to undermine confidence in our democratic institutions and processes, sow divisions in our society, weaken our alliances, and promote their political, economic, or ideological agendas. These entities operate in the seams of our democratic system to advance their interests, using the tools of traditional espionage in combination with cyber operations and influence campaigns.").

seriousness of the problem, in 2017 the Department of Homeland Security ("DHS") designated election infrastructure as critical infrastructure. This includes "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments."[130]

President Obama signed an executive order declaring a national emergency with respect to "significant malicious cyber-enabled activities" and blocking the assets of any person the Secretary of the Treasury determines to be responsible for or complicit in "tampering with, altering, or causing misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions."[131] President Trump signed a similar executive order.[132] Election interference is thus clearly established today as a significant national security threat.

The use of cyber operations and social media to affect elections has a direct impact not only on the federal government but also on U.S. states and localities, which provide the bulk of election infrastructure. In 2019, the Senate Intelligence Committee concluded that Russia had targeted election systems in all fifty states during the 2016 elections, probing for vulnerabilities in the systems.[133] Robert Mueller testified that many other countries were "developing capabilit[ies] to replicate what the Russians have done."[134]

Foreign allies have faced similar interference with their electoral and democratic processes. The UK Parliament's intelligence committee concluded that Russia may have interfered in the 2016 Brexit referendum.[135] The European Union determined that Russia undertook a

[130] Press Release, Dep't of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical [https://perma.cc/PZ94-58JB].

[131] Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016).

[132] See Exec. Order No. 13,848, 83 Fed. Reg. 46,843 (Sept. 12, 2018).

[133] David E. Sanger & Catie Edmondson, Russia Targeted Election Systems in All 50 States, Report Finds, N.Y. Times (July 25, 2019), https://www.nytimes.com/2019/07/25/-us/politics/russian-hacking-elections.html [https://perma.cc/89AT-R3PF].

[134] Id.

[135] Adam Taylor, Did Russia Interfere in Brexit?: An Unpublished Report Roils U.K. Politics Before Election, Wash. Post (Nov. 5, 2019, 10:14 AM), https://www.washington-

"'continued and sustained' disinformation campaign" against its parliamentary elections in 2019.[136] The Baltic states have wrestled with Russian election interference for years.[137] Most recently, Australia's domestic spy agency announced that it was investigating whether China attempted to install an agent in the Australian parliament.[138] As discussed further *infra*, the United States is working closely with foreign allies to share information about election threats and strategies to address the problem, because they face some of the same adversaries and tactics.[139]

3. Terrorism

Terrorism also remains a critical threat to U.S. national security. The September 11 attacks highlighted the power that non-state actors had to inflict damage and trigger fear inside the United States. The federal government played the dominant role in responding to those attacks, using the U.S. military and intelligence community and even creating a new Department of Homeland Security and Office of the Director of National Intelligence to help secure the country. Nevertheless, the Executive also turned to state and local officials to assist the federal government in conducting surveillance and profiling.[140] Today, the federal government continues to rely on a range of partnerships to address the terrorist threat. The 2018 U.S. National Strategy for Counterterrorism emphasized the importance of "relying on our allies to degrade and maintain persistent pressure against terrorists," and, on the domestic front, "empower[ing] our frontline defenders—our state and local law enforcement professionals—as well as many other government, civil

post.com/world/2019/11/05/did-russia-interfere-brexit-an-unpublished-report-roils-uk-politics-before-election/ [https://perma.cc/S5YS-SC83].

[136] Michael Birnbaum & Craig Timberg, E.U.: Russians Interfered in Our Elections, Too, Wash. Post (June 14, 2019, 4:18 PM), https://www.washingtonpost.com/technology/-2019/06/14/eu-russians-interfered-our-elections-too/ [https://perma.cc/8JNZ-7KWH].

[137] Oliver Backes & Andrew Swab, Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States, at v (2019), https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states [https://perma.cc/K4M9-58MV].

[138] Colin Packham, Australia To Probe Foreign Interference Through Social Media Platforms, Reuters (Dec. 5, 2019, 12:45 AM), https://www.reuters.com/article/us-australia-politics/australia-to-probe-foreign-interference-through-social-media-platforms-idUSKBN1-Y90E6 [https://perma.cc/YG6L-YAGX].

[139] See infra Subsection II.B.3.

[140] Waxman, supra note 15, at 291.

society, and private sector partners to prevent and counter terrorism in the United States."[141]

The importance of non-federal actors in defending against domestic terrorism is potentially even more important today, as the terrorist threat shifts from foreign terrorist organizations that attack U.S. assets overseas to "homegrown" jihadist terrorism, including ISIS-inspired actors inside the United States.[142] The FBI Director recently testified that the FBI engages daily with state and local law enforcement authorities regarding threats and trends in the behavior of domestic terror suspects.[143] Two hundred Joint Terrorism Task Forces around the country facilitate this intelligence sharing.[144] At the same time, the United States is "working extensively with its partners in the Five Eyes Alliance . . . and with other countries to tackle this threat."[145] Thus, as with cyber attacks, supply chain threats, and election interference, the federal government must rely on non-federal actors such as state and local law enforcement and foreign allies to help it manage terrorism.

B. The Rise of Unsung Secrecy Surrogates

The novel threats that the Executive faces have forced it to engage with a new set of actors that are in close proximity to—and sometimes direct victims of—these threats. This Section describes in greater detail how these interactions play out and demonstrates how the interactions create the opportunity for these non-traditional actors to serve as our secrecy surrogates. That is, technology companies, states and localities, and

[141] President Donald J. Trump, White House, National Strategy for Counterterrorism of the United States of America, at II (2018), https://www.whitehouse.gov/wp-content/-uploads/2018/10/NSCT.pdf [https://perma.cc/FP65-MTE5]. The United States also must work with telecommunications companies and internet service providers to gain access to telephony metadata and email content under FISA authorities. See Foreign Intelligence Surveillance Act, 50 U.S.C. § 1805 (2012); Foreign Intelligence Surveillance Act Amendments Act § 702, 50 U.S.C. § 1881a (2012). Further, it works with banks to enforce prohibitions on terrorist financing. U.S. Dep't of the Treasury, Terrorist Finance Tracking Program: Questions and Answers, https://home.treasury.gov/system/files/246/Terrorist-Finance-Tracking-Program-Questions-and-Answers.pdf [https://perma.cc/6PYL-B5YK] (last visited Oct. 12, 2020).

[142] Peter Bergen, David Sterman & Melissa Salyk-Virk, New Am., Terrorism in America 18 Years After 9/11, at 29–31 (2019), http://www.newamerica.org/international-security/-reports/terrorism-america-18-years-after-911/ [https://perma.cc/2G58-UST6].

[143] Ford, supra note 107.

[144] Id.

[145] Id.

foreign allies can challenge cases of executive incompetence or illegality and serve as an audience that can force the Executive to improve the quality of its intelligence and justify its classified decisions.[146]

1. Technology Companies

Technology companies interact with sensitive government national security operations in at least three ways. First, during their ordinary course of business, these companies frequently unearth information that directly implicates U.S. national security interests.[147] In some cases, the companies develop threat information that the government itself may not have. Second, the tech companies sometimes receive classified intelligence from the government and are expected to act on it, as when the government shares cyber threat intelligence so that the companies can take steps to protect critical infrastructure. Finally, the government reportedly sometimes asks these companies to incorporate U.S. intelligence into their public cyber security reports. These interactions create a dialogic relationship between the Executive and a subset of sophisticated technology company officials about classified operations.

a. Company-Generated Sensitive Information

The first way in which tech companies confront sensitive information is when they investigate and discover state-directed cyber attacks in the course of their business. In their efforts to protect their clients, cybersecurity companies such as FireEye/Mandiant research, identify, and attribute malicious cyber operations.[148] In this process, they have

[146] See supra Section I.A.

[147] Much of the sensitive information that tech companies encounter or unearth is not "secret" as that term is used in the executive order regulating the classification of government information. Nevertheless, the information may be secret in the informal sense, and in any case often will implicate sensitive U.S. foreign relations issues. See Eichensehr, Public-Private Cybersecurity, supra note 23, at 493–94 ("Mandiant, CrowdStrike, and the other companies that have accused foreign governments of intrusions are engaged in private intelligence-gathering at a sophisticated level."); Dep't of Homeland Sec. & Dep't of Just., Private and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015, at 17 (2018), https://www.us-cert.gov/sites/default/files/ais_files/Privacy_and_Civil_Liberties_Guidelines.pdf [https://perma.cc/WTT5-PN8B] (discussing situations in which the government determines that "cyber threat indicator[s]," which companies can provide to the government, may contain "classified or other sensitive national security information").

[148] See, e.g., Mandiant, APT1: Exposing One of China's Cyber Espionage Units 2 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf [https://perma.cc/Y7KP-ZRZ8]. Companies such as Google also alert their users to state-

released reports naming state actors (including Russia, China, North Korea, and Iran) or their proxies as the source of those operations.[149] In some cases, the companies unearth information that the U.S. intelligence community lacks.[150] For example, in the context of attributing the WannaCry attack, a DNI official stated that "private-sector researchers had detailed data on the cyberattack that they shared with DHS and the intelligence community."[151] She noted, "We relooked at that data that came from the private sector and I think realized what we had," conceding that "[t]he U.S. government does not have the monopoly on intelligence when it comes to cybersecurity."[152] In other cases, companies issue public reports that stand in tension with what the executive branch has asserted about particular national security threats. In September 2020, for instance,

sponsored hacking efforts. Catalin Cimpanu, In Just 3 Months, Google Sent 12k Warnings About Government-Backed Attacks, ZDNet (Nov. 26, 2019, 7:40 PM), https://www.zdnet.com/article/in-just-three-months-google-sent-12k-warnings-about-government-backed-attacks/ [https://perma.cc/38FN-UE6Z].

[149] See Kristen Eichensehr, The Private Frontline in Cybersecurity Offense and Defense, Just Sec. (Oct. 30, 2014), https://www.justsecurity.org/16907/private-frontline-cybersecurity-offense-defense/ [https://perma.cc/U4PQ-TM7F] (arguing that these companies effectively act like governments, identifying national security threats from foreign governments and in some cases defending against those threats); Patrick Howell O'Neill, Inside the Microsoft Team Tracking the World's Most Dangerous Hackers, MIT Tech. Rev. (Nov. 6, 2019), https://www.technologyreview.com/s/614646/inside-the-microsoft-team-tracking-the-world-s-most-dangerous-hackers/ [https://perma.cc/C9KZ-DL7T].

[150] Shane Harris, Google's Secret NSA Alliance: The Terrifying Deals Between Silicon Valley and the Security State, Salon (Nov. 16, 2014, 4:58 PM), https://www.salon.com/2014/11/16/googles_secret_nsa_alliance_the_terrifying_deals_between_silicon_valley_and_the_security_state/ [https://perma.cc/5NRR-7BYX] ("Shortly after the Google breach, Mandiant disclosed the details of its investigations in a private meeting with Defense Department officials a few days before speaking publicly about it.").

[151] Derek Hawkins, The Cybersecurity 202: 'We Have to Work Together.' Government Struggling with Sharing Cyberthreat Information, Officials Say, Wash. Post (July 23, 2018, 7:56 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/07/23/the-cybersecurity-202-we-have-to-work-together-government-struggling-with-sharing-cyberthreat-information-officials-say/5b5496c31b326b1e646954bf/ [https://perma.cc/B8VZ-G4ZM].

[152] Id.; see also O'Neill, supra note 149 (discussing how Microsoft possesses important cyber threat information that the government lacks); Jay Greene, Tony Romm & Ellen Nakashima, Iranians Tried To Hack U.S. Presidential Campaign in Effort That Targeted Hundreds, Microsoft Says, Wash. Post (Oct. 4, 2019, 5:38 PM), https://www.washingtonpost.com/technology/2019/10/04/iran-tried-hack-us-presidential-candidates-journalists-effort-that-targeted-hundreds-microsoft-finds/ [https://perma.cc/CD6J-K8C7] ("Microsoft software is present in far more computers around the world than U.S. law enforcement and intelligence agencies, giving the company a broader window into the threat than government authorities.").

Microsoft issued a report warning that Russian military intelligence was aggressively hacking both Democratic and Republican campaign staff and that China was focused on hacking Democratic candidate Joseph Biden's staff rather than President Trump's. These findings raise questions about executive claims that China was the bigger threat to elections than Russia and that China favored Biden to win the 2020 election.[153] Microsoft's assessment, which was "far more detailed" than those made public by U.S. intelligence agencies, "complicates the administration's narrative."[154]

Three other episodes illustrate this point. First, in 2010, Google's engineers, suspecting that Chinese intruders had penetrated their users' Gmail accounts, gained access to a computer in Taiwan that seemed to be the source of the attacks.[155] On that computer, the engineers discovered evidence of the attacks against Google, but also detected attacks against at least thirty-three other companies, including Adobe and Northrop Grumman. "Seeing the breadth of the problem, they alerted American intelligence and law enforcement officials and worked with them to assemble powerful evidence that the masterminds of the attacks were not in Taiwan, but on the Chinese mainland."[156] More recently, in January 2019, CISA issued an Emergency Directive to address ongoing incidents that involved tampering with the global Domain Name System infrastructure; CISA reportedly learned about the threat from several cybersecurity companies.[157] Finally, in a case in which the FBI shared

[153] David E. Sanger & Nicole Perlroth, Russian Intelligence Hackers Are Back, Microsoft Warns, Aiming at Officials of Both Parties, N.Y. Times (Sept. 10, 2020), https://www.nytimes.com/2020/09/10/us/politics/russian-hacking-microsoft-biden-trump.-html [https://perma.cc/4NF7-H49K] (noting that firms such as "Microsoft and Google, because they sit atop global networks, have a front-seat view of suspicious activity, and increasing motivation to make it public to warn their customers").

[154] Id.

[155] David E. Sanger & John Markoff, After Google's Stand on China, U.S. Treads Lightly, N.Y. Times (Jan. 14, 2010), https://www.nytimes.com/2010/01/15/world/asia/15diplo.html [https://perma.cc/XUN7-AV3C].

[156] Id.

[157] CISA, CISA Emergency Directive on DNS Infrastructure Tampering (Jan. 25, 2019), https://us-cert.cisa.gov/ncas/current-activity/2019/01/22/CISA-Emergency-Directive-DNS-Infrastructure-Tampering [https://perma.cc/4F9A-RBHS]; Muks Hirani, Sarah Jones & Ben Read, Global DNS Hacking Campaign: DNS Record Manipulation at Scale, FireEye (Jan. 10, 2019), https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html [https://perma.cc/3WMU-DQNJ]; see also Harris, supra note 150 (reporting that McAfee provides the NSA, CIA, and FBI with "network traffic flows, analysis of malware, and information about hacking trends"). This type of relationship

with banks the cases it was tracking, the banks already were aware of all but one of those cases and effectively confirmed the FBI's intelligence.[158] These incidents collectively illustrate that companies and the government have extensive, non-public conversations about cyber threat detection and attribution, and that the companies are sometimes the original source of threat information.

b. Companies as Recipients of Government Intelligence Sharing

The Executive also reveals classified information to tech companies. It does so not simply to enable the companies to provide other forms of information back to the government, such as when the government shares classified identifier information with telecommunications providers so that they can turn over certain communications under U.S. electronic surveillance laws.[159] The Executive also reveals the information so that the tech companies themselves can directly act on the intelligence to protect their clients, which are often U.S. citizens or companies.[160]

A tangle of statutes and executive orders contemplates that the government will share cyber-related intelligence with the private sector, including certain classified information.[161] In 2015, President Obama issued an executive order that called for the creation of Information Sharing and Analysis Organizations ("ISAOs") to improve cybersecurity information sharing between the government and the private sector. Executive Order 13,691 provides that the Secretary of Homeland Security "will determine the eligibility of ISAOs and their members for any

exists in other countries as well. For example, ProtonMail worked with Swiss authorities to help shut down cyber attacks from actors reportedly associated with Russia's intelligence directorate. Sam Jones, Cyber Attack Hits Email Users Probing Russian Intelligence, Fin. Times (July 26, 2019), https://www.ft.com/content/876fb2d8-af92-11e9-8030-530adfa879c2 [https://perma.cc/F9NE-PU3M].

[158] Harris, supra note 110, at 167–68.

[159] See, e.g., Foreign Intelligence Surveillance Act Amendments Act of 2008 § 702, 50 U.S.C. § 1881a (2012); USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, 269–70.

[160] See Eichensehr, Public-Private Cybersecurity, supra note 23, at 496–97 ("The basic system that has evolved for securing critical infrastructure systems from cybersecurity breaches casts the private sector as the main actor—either companies defend their own networks, or they hire other companies to do so—and the government plays only a supporting role.").

[161] For an overview of cybersecurity information sharing as of March 2015, see Andrew Nolan, Cong. Rsch. Serv., R43941, Cybersecurity and Information Sharing: Legal Challenges and Solutions 6–12 (2015), https://fas.org/sgp/crs/intel/R43941.pdf [https://perma.cc/7XPV-6DQ2].

necessary facility or personnel security clearances associated with voluntary agreements."[162] Late in 2015, Congress passed the Cybersecurity Information Sharing Act,[163] which required U.S. national security agencies to establish procedures for the "timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances."[164] The government also created the National Cyber Investigative Joint Task Force, which "provides classified threat briefings to . . . cleared private sector representatives."[165] Further, the "FBI utilizes on-site briefings to share classified indicators and defensive measures with industry and appropriate private sector entities."[166] The FBI provides victims with temporary security clearances so they can have access to "specific classified information and technical indicators that may be used to neutralize an ongoing threat," and often "the technical information exchanged is accompanied by a contextual briefing to emphasize the severity of the threat."[167] Finally, the FBI provides classified briefings on cybersecurity best practices.[168]

DHS also shares classified information with companies. A program within the DHS-led National Cybersecurity and Communication Integration Center shares classified government cyber threat information with some private actors (such as telecommunications companies), which then can detect and block malicious cyber traffic to their own systems and those of their commercial clients.[169] Further, under DHS's Cyber

[162] Exec. Order No. 13,691, § 4(c), 80 Fed. Reg. 9349 (Feb. 13, 2015).

[163] Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1502–33 (2018).

[164] Id. § 1502(a)(1). CISA also envisions that the executive will declassify and share at the unclassified level information related to cyber security threats. Id. § 1502(a)(2). And it provides that non-federal entities receiving cyber threat indicators shall comply with lawful restrictions placed on the use of that information and use security controls to "protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures." Id. §§ 1502(b)(1)(D), 1503(c)(2).

[165] Off. of the Dir. of Nat'l Intel. et al., supra note 12, at 8–9.

[166] Id. at 9.

[167] Id.

[168] Id. at 16.

[169] See Nolan, supra note 161, at 6–8; Exec. Order No. 13,636, § 4(c), 78 Fed. Reg. 11,739 (Feb. 12, 2013) ("To assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm, the Secretary . . . shall . . . establish procedures to expand the Enhanced Cybersecurity Services program to all critical infrastructure sectors. This voluntary information sharing program will provide classified cyber threat and technical information from the Government to eligible

Information Sharing and Collaboration Program, companies may sign cooperative research agreements and receive access to an intelligence integration center, and corporate personnel eligible for security clearances can receive classified threat information.[170] In the election security setting, senior officials from DHS met with state and local election officials and private sector election companies to hold "a classified briefing on the current cyber threat landscape" for the 2018 elections.[171] Although some critics have complained that executive branch classified threat sharing has been too limited, there have been a host of cases in which the government has shared information with cleared individuals at private companies.[172]

In order to share classified information with the private sector, the government will often provide temporary (or permanent) security clearances to technology company officials who have a "need to know." Beginning in 2008, the government began offering tech company executives temporary clearances, "some good for only one day, so they could sit in on classified threat briefings."[173] In the Google incident related to China-based hacking discussed *supra*, the government gave Sergey Brin, Google's co-founder, a temporary security clearance so that

critical infrastructure companies or commercial service providers that offer security services to critical infrastructure."); CISA, Enhanced Cybersecurity Services (ECS) (Mar. 6, 2019), https://www.dhs.gov/cisa/enhanced-cybersecurity-services-ecs [https://perma.cc/6-FAZ-2A8Q] (describing "Enhanced Cybersecurity Services"); Joseph Menn, Government To Share Cyber Security Information with Private Sector, Ins. J. (May 15, 2013), https://www.insurancejournal.com/news/national/2013/05/15/292065.htm [https://perma.cc/-53VN-AAY7] (describing system by which the National Security Agency and other intelligence agencies provide attack signatures to service providers with security clearances, such as telecommunications and defense companies, which then screen out malicious traffic to clients such as "utilities, banks and other critical infrastructure companies that choose to pay for them").

[170] Off. of the Dir. of Nat'l Intel. et al., supra note 12, at 8.

[171] Press Release, Dep't of Homeland Sec., DHS Holds Classified Briefing for Private Sector Election Companies (Oct. 2, 2018), https://www.dhs.gov/news/2018/10/02/dhs-holds-classified-briefing-private-sector-election-companies [https://perma.cc/G2UZ-QK3X] (describing a "trusted public-private partnership to share threat information, exchange best practices, and collaborate on exercises and incident planning" and the "growing partnership between DHS and the election sector").

[172] Robert K. Knake, Sharing Classified Cyber Threat Information with the Private Sector, Council on Foreign Rels. (May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector [https://perma.cc/L3PX-U88S] (arguing that the government should revamp security clearance rules for tech company employee clearances).

[173] Harris, supra note 150.

he could attend a classified briefing about the campaign against Google.[174]

These are not the only contexts in which the Executive shares classified threat information with technology companies and other private actors. Then-Director of National Intelligence Dan Coats and other senior intelligence officials briefed technology companies, venture capitalists, and educational institutions on the dangers of doing business with China.[175] In the briefings, which also discussed intellectual property theft, the intelligence community showed the executives classified information.[176] The leader of a tech company consortium praised the interactions, stating, "It is a great thing that the intelligence community and law enforcement [are] interacting and engaging with the private sector in this way—executives say they have found it very useful."[177] Further, the government and tech companies have engaged in closed-door discussions about threats to the 2020 election.[178]

c. Companies as Fronts for Publicizing Intelligence

A third setting in which technology companies interact with classified information is when the government provides it to cyber security companies to assist in the companies' public attributions.[179] The U.S. government reportedly gave Mandiant information that the latter used in its report identifying Advanced Persistent Threat 1 ("APT1") as a Chinese government entity, and the government apparently gave CrowdStrike technical information that the latter used in attributing the OPM hack to

[174] Id.

[175] Kiran Stacey & Demetri Sevastopulo, US Spy Chiefs Warn Tech Companies on China Dangers, Fin. Times (May 19, 2019), https://www.ft.com/content/dde4f848-78ed-11e9-be7d-6d846537acab [https://perma.cc/E7VA-VANF]; James Vincent, US Spy Chiefs Used Classified Info To Warn Tech Execs About Doing Business with China, Verge (May 20, 2019, 5:47 AM), https://www.theverge.com/2019/5/20/18632236/us-spy-chiefs-brief-silicon-valley-tech-execs-danger-business-china [https://perma.cc/PD6P-LVWZ].

[176] Stacey & Sevastopulo, supra note 175.

[177] Id.

[178] Tony Romm & Ellen Nakashima, U.S. Officials Huddle with Facebook, Google and Other Tech Giants To Talk About the 2020 Election, Wash. Post (Sept. 4, 2019, 7:31 PM), https://www.washingtonpost.com/technology/2019/09/04/us-officials-huddle-with-facebook-google-other-tech-giants-talk-about-election/ [https://perma.cc/2ZGA-RU38] (describing a meeting among DHS, DNI, FBI, Facebook, Google, Microsoft, and Twitter and noting that the companies declined to discuss what they talked about).

[179] See Kristen E. Eichensehr, Decentralized Cyberattack Attribution, 113 AJIL Unbound 213, 215 (2019).

China.[180] In these cases, the government shares classified information with particular tech companies with the intent that the companies will use the information to make attributions that the government wants them to make, but does not want to make itself (at least at that time). The companies effectively "launder" the information for the government, presumably because the public sees the companies as more neutral and objective than the Executive.[181] At the same time, if the companies disagree with the intelligence that the government provides them, they presumably decline to rely on it in their reports.

d. Government/Company Interactions as Checks

The technology companies' ability to develop "intelligence" about cyber and election threats and receive classified information about threats and responses allows them to act as a direct external check on the Executive, while also stimulating Congress to conduct oversight. Some tech companies are very sophisticated consumers of government intelligence and know more than the government about particular cyber operations. In addition, their employees are often former intelligence community officials who understand how U.S. intelligence analysis and operations work.[182] Further, tech companies have broad visibility into cyber operations and are positioned to detect certain offensive operations that the United States may undertake—something the U.S. government is aware of. This means that the tech company officials might even be better positioned than certain executive actors, such as those from the State or Treasury Departments, to critique intelligence information or plans.[183] There are reported cases in which the tech companies have directly challenged and checked executive conclusions about the intelligence they

[180] Id. at 215 n.17.

[181] In the Google/China episode discussed above, the positions of the government and companies were effectively reversed, with Google's unclassified revelations about Chinese hacking enabling the government to discuss the issue publicly "'without having to rely on classified sources or sensitive methods' of intelligence gathering." Harris, supra note 150.

[182] See Tim Shorrock, How Private Contractors Have Created a Shadow NSA, Nation (May 27, 2015), https://www.thenation.com/article/how-private-contractors-have-created-shadow-nsa/ [https://perma.cc/8XR6-HQMM] (describing how a host of former high-level U.S. intelligence officials have migrated to companies that contract with the National Security Agency and other intelligence agencies).

[183] See Deeks, Checks and Balances, supra note 9, at 83.

receive.[184] The *Wall Street Journal* reported, for example, that at a classified threat briefing by intelligence community leadership, some attendees "pressed the government for hard evidence of the threat."[185] In the cyber threat information sharing setting, stakeholders have complained to Congress that they lacked "confidence in the validity of some indicators [provided to them by the federal government] because of a lack of adequate vetting."[186]

The companies also have demanded more context for the information that the government provides so that they can better evaluate its quality. A former DHS official who later worked at American Express noted:

> Just as the context is important to security analysts, the lack of context prevents users of the information from confirming that the indicators have been properly vetted and received from trustworthy sources. Providing mechanisms for representing and encouraging the supply of additional context, providing real-time feedback on data quality, and supporting different communities of trust are ways to advance the program.[187]

Microsoft's President, Brad Smith, made a similar argument in the supply chain setting. Microsoft asked U.S. regulators to explain their decisions

[184] Maximizing the Value of Cyber Threat Information Sharing: Hearing Before the Subcomm. on Cybersecurity and Infrastructure Prot. of the H. Comm. on Homeland Sec., 115th Cong. 21 (2017) (statement of Ann Barron-Dicamillo, Vice President, Cyber Intel & Incident Response, American Express) (testimony by a former DHS official about how she pressured her DHS employees to declassify more information because companies were not receiving enough context) [hereinafter Cyber Threat Information Sharing]; Rolfe Winkler, Chinese Cash That Powered Silicon Valley Is Suddenly Toxic, Wall St. J. (June 11, 2019, 10:28 AM), https://www.wsj.com/articles/chinese-cash-is-suddenly-toxic-in-silicon-valley-following-u-s-pressure-campaign-11560263302 [https://perma.cc/YD3A-697W]; cf. Goldsmith, supra note 29, at 206–07 (articulating the idea of a presidential synopticon). We might construe the developments discussed here as a cousin of Goldsmith's synopticon, which forced various secret government programs into the light and exposed them to criticism and change. Here, the companies may keep their criticism out of public view to avoid compromising future intelligence sharing by the government.

[185] Winkler, supra note 184.

[186] Cyber Threat Information Sharing, supra note 184, at 8 (statement of Rep. Bennie G. Thompson, Ranking Member, H. Comm. on Homeland Sec.) (noting other complaints by the private sector that "too much of the information necessary to make indicators actionable is Classified").

[187] Id. at 22 (statement of Barron-Dicamillo).

prohibiting Huawei from buying U.S. technology.[188] Smith said that the government would often assert that "if you knew what we knew, you would agree with us." Microsoft's response? "Great, show us what you know so we can decide for ourselves. That's the way this country works."[189] Five Republican senators wrote Smith a letter detailing the publicly available evidence that Huawei poses a national security threat but conceding, "We believe the Federal Bureau of Investigation or the intelligence community could share more of this intelligence in an appropriate fashion to affected businesses."[190]

Technology companies that receive classified information or classified requests for cooperation are poised to challenge not only the quality of the intelligence but also what they perceive as illegal activities. Before the September 11 attacks, Qwest, a U.S. telecommunications company, pushed back on the National Security Agency's request for access to its fiber optic networks "because officials hadn't obtained a court order to get access to the company's equipment."[191] Even after the attacks, Qwest insisted that the government obtain a warrant before it would turn over its phone records.[192] Yahoo and Twitter have both noted that they carefully review government requests for data for legal sufficiency and interpret the requests narrowly.[193] In other cases, the tech companies enable more traditional surrogates to review the legality of executive activity themselves. When tech companies sued to be able to reveal the numbers of FISA orders they received, for instance, their lawsuit empowered the FISC to serve in its traditional role as secrecy surrogate.[194]

This type of intelligence sharing also renders the information a shallower secret because it is being dispersed to an audience that is wider

[188] Dina Bass, Microsoft Says Trump Is Treating Huawei Unfairly, Bloomberg Businessweek (Sept. 8, 2019), https://www.bloomberg.com/news/articles/2019-09-08/microsoft-says-trump-is-treating-huawei-unfairly [https://perma.cc/P8ZN-5LEM].

[189] Id.

[190] Letter from Sens. Tom Cotton, Marco Rubio, Rick Scott, Josh Hawley & Mike Braun, U.S. Senate, to Brad Smith, President, Microsoft (Oct. 7, 2019), https://www.cotton.senate.gov/files/documents/Microsoft.pdf?wpisrc=nl_cybersecurity202&wpmm=1 [https://perma.cc/AKG8-VYKK].

[191] Harris, supra note 110, at 184.

[192] Id.

[193] Rozenshtein, supra note 22, at 125.

[194] See Craig Timberg & Cecilia Kang, Google Challenges U.S. Gag Order, Citing First Amendment, Wash. Post (June 18, 2013), https://www.washingtonpost.com/business/technology/google-challenges-us-gag-order-citing-first-amendment/2013/06/18/96835c72-d832-11e2-a9f2-42ee3912ae0e_story.html [https://perma.cc/WTU6-WNDJ].

and more diverse than the intelligence community itself.[195] Indeed, if a respected tech company published a cyber attribution that was inconsistent with a U.S. government attribution (one that the government either made publicly or shared secretly with the intelligence committees), that inconsistency might stimulate Congress to hold hearings or seek briefings by the Executive on the attribution question and the classified information supporting it.[196] Likewise, if the tech companies receive what they perceive to be flawed intelligence or learn about intelligence programs that they perceive to be unlawful, they might make critical but unclassified comments to the press about their negative experiences with their government interlocutors. This, too, could stimulate Congress to act, and the Executive's knowledge that the tech companies are in position to "watch" them may alter its behavior ex ante.

There is at least one other way that tech companies might serve as "secrecy surrogates" in the cyber context. They might pressure the government not on the substance of its secret conclusions and activities but on the very fact of classification, using litigation or self-disclosure. Corporations have sued, for instance, when they believed that the government was keeping too much information secret about the number of FISA orders it was serving on tech companies.[197] The Justice Department issued a "new binding policy, limiting the use and duration of secrecy orders" in response to Microsoft's victory in litigation.[198] In the Google/China episode discussed *supra*, Google pressed the government for four years to "go public with information about Chinese spying, to shame the country into stopping its campaign."[199] The United States was unwilling to do so, and so Google's chief legal officer

[195] Pozen, supra note 5, at 274.

[196] See Deeks, Checks and Balances, supra note 9, at 84 ("[T]hese technology firms help Congress overcome its informational disadvantages on technology and information about US intelligence-community operations.").

[197] See Kristen E. Eichensehr, Digital Switzerlands, 167 U. Pa. L. Rev. 665, 677–78 (2019) [hereinafter Eichensehr, Digital Switzerlands]; see also id. at 713 ("[C]ompanies are on notice about government demands [which often are secret] in a way that individual users often are not."); Note, Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance, 131 Harv. L. Rev. 1722, 1737–38 (2018); Josh Gerstein, Judge Tosses Twitter Suit Over Surveillance Secrecy, Politico (Apr. 18, 2020, 12:37 PM), https://www.politico.com/news/2020/04/18/federal-judge-dismisses-surveillance-twitter-suit-193557 [https://perma.cc/XJ6Q-MTWF] (discussing Twitter's multi-year effort to force the government to allow it to reveal statistics about the number of FISA warrants and national security letters Twitter receives).

[198] Eichensehr, Digital Switzerlands, supra note 197, at 679.

[199] Harris, supra note 150.

ultimately posted a public statement accusing China of hacking Google's infrastructure.[200] Google's decision to reveal the information was not a leak, because it had acquired the information on its own. More generally, a host of companies have urged the government to declassify and share more threat information, which would convert shallow secrets into information that was no longer classified at all.[201] The companies have done this in part because even if some individuals in a company receive access to classified information, it is hard to convert that information into "actionable" information for use by other, uncleared individuals in the organization.[202] Regardless of the reason, however, companies already have played a role in checking executive judgments about the requisite *levels* of secrecy, in addition to checking the *substance* of secret government analyses or operations.

2. States and Localities

States and localities (which this Article refers to generally as "local governments") play a critical role in helping the federal government defend against cyber threats, election interference, and terrorism. In some cases, local government officials are primarily in "receive" mode, accepting both classified and non-classified information from the federal government about the threats they face. This is particularly true for states and cities that are smaller and less experienced in dealing with national security issues. But these briefings create an opportunity for local government officials, especially those in major cities such as New York, Chicago, and Los Angeles, to probe the substance of the intelligence and the level of confidence the government has in it. The local governments know more about the structure of their own technological and infrastructure systems and the operation of elections than most federal officials do, which creates a significant opportunity for the federal government to glean important information and corrections from local actors. There is precedent for this type of pushback: in certain terrorism cases in which the federal government sought assistance from local governments, those local actors pushed back on the legality of the requests and the underlying information guiding federal strategies.

[200] Id.

[201] See, e.g., Cyber Threat Information Sharing, supra note 184, at 19 (statement of Barron-Dicamillo).

[202] Id. at 19–20.

As a baseline matter, the federal government has created several avenues to provide security clearances to local government officials. In Executive Order 13,549, entitled "Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities," President Obama sought to ensure the security of classified information that the federal government shares with those actors.[203] In the election setting, DHS has worked to declassify or downgrade the classification of election-related threats.[204] The intelligence community provided classified briefings about interference in the 2018 midterm elections to election officials from all fifty states.[205] In those briefings, the intelligence community planned to give the local officials "classified examples of recent attempted and successful interference by hostile parties in U.S. election systems," "discussions of foreign attempts to use social and mainstream media to influence American voters," and "advice on possible security enhancements."[206] Relatedly, DHS has worked with state chief election officials and other election staff to provide them with security clearances[207] or classified one-day "read-ins" to receive intelligence about threats to election infrastructure.[208] In its report on election interference, the Senate Select Committee on Intelligence, which interviewed state

[203] Exec. Order No. 13,549, 75 Fed. Reg. 51,609 (Aug. 18, 2010).

[204] Defending Our Democracy: Building Partnerships To Protect America's Elections: Hearing Before the H. Comm. on Homeland Sec., 116th Cong. 4 (2019) (statement of Christopher Krebs, Dir., Cybersecurity and Infrastructure Security Agency, U.S. Dep't of Homeland Sec.) [hereinafter Krebs]; see also Election Security Preparations: Federal and Vendor Perspectives: Hearing Before the S. Comm on Rules & Admin., 115th Cong. 4 (2018) (statement of Matt Masterson, Senior Cybersecurity Advisor, U.S. Dep't of Homeland Sec.) [hereinafter Masterson] ("By working with ODNI and the [FBI], in February 2018 election officials from each state received one-day read-ins for a classified threat briefing . . . . This briefing demonstrated our commitment to ensuring election officials have the information they need to understand the threats they face.").

[205] Josh Delk, Intel Agencies To Brief Officials from All 50 States on Election Threats, Hill (Feb. 15, 2018, 7:07 PM), https://thehill.com/policy/national-security/374148-intel-agencies-to-brief-officials-from-all-50-states-on-election [https://perma.cc/8KWD-NE7W].

[206] Mark Hosenball, U.S. Spy Agencies To Brief State Officials on Election Threats, Reuters (Feb. 15, 2018, 5:28 PM), https://www.reuters.com/article/us-usa-election-cyber/u-s-spy-agencies-to-brief-state-officials-on-election-threats-idUSKCN1FZ2ZF [https://perma.cc/JFC7-286A].

[207] Krebs, supra note 204, at 4; Masterson, supra note 204, at 4.

[208] Krebs, supra note 204, at 5–6.

election officials, recommended increasing the number of security clearances in each state.[209]

In the cyber setting, local governments have shown some appetite for challenging the federal government's current approach to legal norms for cyberspace. Some U.S. states and localities "are breaking with the federal government and signing onto" the Paris Call, a declaration "aimed at making cyberspace safer."[210] One of the local officials' goals is to pressure the federal government to work with other governments to establish more restrictive rules in cyberspace.[211] As one report notes, the decision to sign onto the Paris Call "underscores how states and localities, which have been pelted with costly ransomware attacks and struggled to protect their elections against highly sophisticated Russian hackers in recent years, are increasingly viewing cybersecurity as an existential threat."[212] While this example reflects a publicly disclosed policy divergence between federal and local actors, one can extrapolate that federal and local officials have also disagreed in closed-door settings about some of the federal government's cyber policies and decisions. This seems especially true for a city such as New York, which has created its own Cyber Command to mitigate cyber threats and collaborate with federal and state officials and the private sector.[213]

A third area in which local officials play an important national security role is in counter-terrorism operations. In the wake of the September 11 attacks, the federal government significantly ramped up its counter-terrorism efforts, recognizing that it required much greater levels of information and assistance from local officials and foreign governments.[214] On the domestic front, President Bush ordered the federal government to "give the highest priority" to "the interchange of terrorism

[209] S. Select Comm. on Intel., Report on Russian Active Measures Campaigns and Interference, S. Rep. No. 116-XX, at 55–56 (2019), https://www.intelligence.senate.gov/-sites/default/files/documents/Report_Volume1.pdf [https://perma.cc/C54L-H22T].

[210] Joseph Marks & Tonya Riley, The Cybersecurity 202: States and Cities Make Cybersecurity Pledge After Trump Administration Rejects It, Wash. Post (Nov. 15, 2019, 7:33 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/15/the-cybersecurity-202-states-and-cities-make-cybersecurity-pledge-after-trump-administration-rejects-it/5dcd8c2388e0fa10ffd20e7d/ [https://perma.cc/GA9U-TEWM].

[211] Id.

[212] Id.

[213] City of New York, Exec. Order No. 28 (July 11, 2017), https://www1.nyc.-gov/assets/home/downloads/pdf/executive-orders/2017/eo_28.pdf [https://perma.cc/7CNG-HAMH].

[214] Waxman, supra note 15, at 302; Ford, supra note 107.

information between agencies and appropriate authorities of State, local, and tribal governments."[215] The federal government recognized that often those entities "are best able to identify potential threats that exist within their jurisdictions" because local police are more familiar with their communities and can better cultivate sources of information, especially where suspected terrorists are operating inside the United States.[216]

One way that the federal government operationalized this cooperation was by creating dozens of Joint Terrorism Task Forces ("JTTFs"). These JTTFs are led by the FBI and consist of federal, state, and local officials assigned to "help coordinate intelligence and law enforcement operations across bureaucratic lines."[217] Some local government participants in JTTFs have security clearances and receive classified threat information.[218] DHS also funds state-run "fusion centers" that compile and route terrorism-related law enforcement and investigative information, and that can receive classified intelligence from federal partners.[219] The National Counterterrorism Center established a Joint Counterterrorism Assessment Team, whose members include state and local first responders who help distill federal terrorism-related information into a usable format that is, "to the extent possible, unclassified, to facilitate further dissemination."[220] Further, major cities

[215] Exec. Order 13,388, § 1(a), 70 Fed. Reg. 62,023 (Oct. 25, 2005).

[216] Inspectors Gen. of the Intel. Cmty., Dep't of Homeland Sec. & Dep't of Just., Review of Domestic Sharing of Counterterrorism Information 6 (2017), https://www.dni.gov/files/-documents/Newsroom/Domestic_Sharing_Counterterrorism_Information_Report.pdf [https://perma.cc/MT4R-R37M]; Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 390, 401–02 (2004), https://www.9-11commission.gov/report/-911Report.pdf [https://perma.cc/E458-F2ES]; Waxman, supra note 15, at 304, 326.

[217] Waxman, supra note 15, at 308.

[218] FBI, Security Clearances for Law Enforcement, https://www.fbi.gov/resources/law-enforcement/security-clearances-for-law-enforcement [https://perma.cc/925C-JM8X] (last visited July 26, 2020).

[219] Waxman, supra note 15, at 308–09; Dep't of Homeland Sec., National Network of Fusion Centers Fact Sheet, https://www.dhs.gov/national-network-fusion-centers-fact-sheet# [https://perma.cc/QG2Y-CMAY] (last visited July 26, 2020). The federal government also shares classified counter-terrorism information with local actors through the Interagency Threat Assessment and Coordination Group. See 6 U.S.C. § 124k (2018); Dep't of Homeland Sec., Implementing Directive: Classified National Security Information Program for State, Local, Tribal and Private Sector Entities (2012), https://www.dhs.gov/sites/default/files/-publications/mgmt-classified-national-security-program-implementation-directive.pdf [https://perma.cc/5TLL-NA83].

[220] Off. of Dir. of Nat'l Intel., About Us—Joint Counterterrorism Assessment Team, https://www.dni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team [https://perma.-cc/DV9K-UMJK] (last visited July 26, 2020). Part of the Team's responsibility is to "[a]dvise

such as New York have established their own counter-terrorism task forces, which engage in very sophisticated collection and operations, even as they cooperate with federal actors and foreign governments.[221]

As Part III discusses, these activities—and the opportunities they present for local officials to challenge classified federal activities—represent federalism in action. As Matthew Waxman notes:

> [S]ome friction between intelligence agencies at various levels of government resulting from these distinctive institutional perspectives may be useful for combating the "groupthink" and politicization of intelligence that can occur within entirely unified structures. . . . [E]ven when they cooperate, they provide localized feedback based on contextualized experience and community reactions to federal initiatives.[222]

Further, "the need for officials at one level of government to persuade officials at the other can . . . serve a checking function."[223] Waxman describes a number of cases in which local officials pushed back on federal requests for counter-terrorism assistance or data-sharing initiatives because they viewed the proposed federal actions as either unlawful or unwise.[224] In short, when the federal government must engage with local officials in order to fully accomplish its goals, those local officials gain power to challenge federal activity, even (or perhaps especially) in settings that involve classified intelligence and programs.

3. Foreign Allies

The United States also undertakes robust intelligence sharing and joint (classified) operations with foreign allies in the cyber, elections, and terrorism contexts. As Aiden Wills and Hans Born write, "The scope, scale and significance of [intelligence] cooperation have increased exponentially over the past two decades, and particularly since 2001.

and make recommendations to the Intelligence Community on how to tailor its products to satisfy the needs of" state and local intelligence consumers. Id.

[221] NYPD, Counterterrorism, https://www1.nyc.gov/site/nypd/bureaus/investigative/-counterterrorism.page [https://perma.cc/8SPJ-4DMP] (last visited July 26, 2020). For Los Angeles, see LAPD, Counter-Terrorism and Special Operations Bureau, http://www.lapdonline.org/inside_the_lapd/content_basic_view/6502 [https://perma.cc/UJ3J-GRL7] (last visited July 26, 2020).

[222] Waxman, supra note 15, at 333.

[223] Id.

[224] Id. at 316–17.

Globalisation has facilitated the proliferation of transnational threats which have induced intelligence services to cooperate with a broader range of international contemporaries on an ever-greater range of issues."[225] The U.S. intelligence community cooperates most closely with its Five Eyes partners (Canada, UK, Australia, and New Zealand), as well as NATO allies and other states with which it has less formalized relationships. In some cases, the United States shares intelligence with an even broader set of states, including through UN bodies such as the International Atomic Energy Agency[226] and the Security Council.[227]

A substantial part of this cooperation—and the exchange of classified information—has been driven by the threat of terrorism by non-state actors. In the post-9/11 era, the United States, working with partners, set up Counterterrorist Intelligence Centers in two dozen countries, from which they "worked together to track and capture suspected terrorists and to destroy or penetrate their networks."[228] In its 2018 Counterterrorism Strategy, the United States continued to emphasize the important roles that its allies and partners play in shared counterterrorism efforts, which often implicate classified information and operations.[229]

Cooperation with allies is escalating in the cyber realm, notwithstanding the fact that states often treat their cyber capabilities as highly sensitive. The United States reportedly cooperated with Israel to

[225] Aiden Wills & Hans Born, International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions, *in* International Intelligence Cooperation and Accountability, supra note 39, at 277.

[226] See Jeffrey T. Richelson, The U.S. Intelligence Community 375 (7th ed. 2016) (describing U.S. sharing of satellite imagery with IAEA to "convince members that North Korea was violating its commitments under the Nuclear Nonproliferation Treaty," and stating that IAEA inspectors ended up taking action on that intelligence, suggesting that they concluded that it was credible); see also Simon Chesterman, Lowy Inst., Shared Secrets: Intelligence and Collective Security 26 (2006), https://warwick.ac.uk/fac/soc/pais/-people/aldrich/vigilant/chesterman_shared_secrets_2006.pdf [https://perma.cc/4UDD-EC3T] (noting that the "IAEA lacks a collection capacity as such, but employs experts who are able to assess information in their possession"). IAEA has protocols for handling states' classified info.

[227] See S.C. Res. 1735, Annex I (Dec. 22, 2006) (providing a cover sheet for submitting names to the sanctions committee, which requires states to provide a specific basis and a "statement of the case" for listing an individual or group and allows states to decide what portions of the statement, if any, the committee may release to the public or member states).

[228] Richelson, supra note 226, at 389; DeVine, supra note 71, at 6.

[229] National Strategy, supra note 141, at 2; DeVine, supra note 71, at 2–3, 6 (describing the U.S. intelligence community's extensive foreign intelligence relationships and the role 9/11 played in expanding those relationships).

develop and execute a covert cyber operation against Iran.[230] The head of U.S. Cyber Command testified that it "has been active with current and prospective foreign partners, especially countries contemplating or building their own cyber forces."[231] He also noted that officials of some "Five Eyes" partners are integrated into the Command's staff and that in fiscal year 2018, Cyber Command "conducted bilateral cyber exercises with France, Estonia, and Japan, while two dozen countries sent observers to our annual CYBER FLAG exercise last June."[232] On the multilateral front, NATO is working to pool its member states' offensive cyber capabilities to respond to cyber threats from state-backed hackers.[233]

The United States also has begun to work bilaterally with states that face threats to their elections, including Montenegro, which faced cyber attacks in advance of its 2016 elections and accession to NATO.[234] U.S. Cyber Command's statement about that cooperation noted that the partnership's operations "generate[d] insights into adversarial cyber threats to the upcoming U.S. and Montenegrin elections in 2020,"[235] and U.S. Secretary of State Mike Pompeo said that as the result of the cooperation, the two countries have developed ways to counter the latest Russian malware.[236] Foreign allies also provide the United States with critical intelligence about attacks on our elections. The Dutch reportedly gained access to Russia's election interference operations and provided

[230] See 50 U.S.C. § 3093(a)(4) (2012) (contemplating involvement in covert action of third parties that are "not an element of, or a contractor or contract agent of, the United States Government").

[231] Statement of Gen. Paul M. Nakasone, Commander, U.S. Cyber Command, Before the S. Comm. on Armed Servs. (Feb. 14, 2019), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf [https://perma.cc/YR9L-SGUV].

[232] Id.

[233] Shannon Vavra, NATO Cyber-Operations Center Will Be Leaning on Its Members for Offensive Hacks, Cyberscoop (Aug. 30, 2019), https://www.cyberscoop.com/nato-cyber-operations-offensive-hacking-neal-dewar/ [https://perma.cc/PNA6-9ZM9].

[234] Dusan Stojanovic, US, Montenegro Plot Cyber Warfare Ahead of 2020 Elections, Associated Press (Nov. 19, 2019), https://apnews.com/article/37456bb4d1b7435395acc4e8be56851b [https://perma.cc/B34Z-LDBJ]; Shannon Vavra, Pentagon Again Deploying Cyber Personnel Abroad To Gather Intel for 2020 Elections, Cyberscoop (Nov. 1, 2019), https://www.cyberscoop.com/pentagon-deploying-cyber-personnel-abroad-gather-intel-2020-elections/ [https://perma.cc/VVV6-BRZV] (discussing U.S. cooperation with North Macedonia, Montenegro, and Ukraine); Sean Lyngaas, Cyber Command's Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia, Cyberscoop (Mar. 14, 2019), https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/ [https://perma.cc/F2JD-E8GV].

[235] Stojanovic, supra note 234; Vavra, supra note 234.

[236] Vavra, supra note 234.

key intelligence about the role of those operations in the 2016 U.S. election.[237] The United States gave the Dutch technology and intelligence in return.[238] These examples of cooperation reveal a two-way exchange of information and tactics in a classified setting.[239]

In these settings, foreign partners are positioned to challenge the quality of U.S. intelligence, the legality of secret operations, and U.S. policy choices.[240] Foreign allies' intelligence services possess "a granular understanding of operations, technologies, and techniques that those who are not intelligence professionals lack."[241] Importantly, these allies care about accuracy, because—as discussed in Part III—inaccurate intelligence directly and adversely impacts their own security.[242] In some cases, therefore, allies have both the expertise and the incentives to press the U.S. intelligence community and the U.S. military about the quality of the intelligence that the United States shares. Particularly in close intelligence relationships, "the commentary and analysis presented by allied analysts can improve [the U.S.] understanding of foreign developments."[243] In the Five Eyes setting, the heads of national assessment "meet at least annually" and "[i]nter-agency is routine at working levels, where the default inclination is to consult widely before assessments are finalized."[244]

In several recent, public episodes, the United States has shared intelligence with foreign allies and has seen those allies contest its

[237] Modderkolk, supra note 128 (describing how Dutch intelligence penetrated Cozy Bear's system, as well as its physical location, by hacking cameras inside the location).

[238] See id.

[239] DeVine, supra note 71, at 13 ("Intelligence sharing may help to corroborate U.S. national sources in addition to possibly providing unique information.").

[240] For an example of a "policy" check, see Richard J. Aldrich, British Intelligence and the Anglo-American "Special Relationship" During the Cold War, 24 Rev. Int'l Stud. 331, 340–41 (1998) (discussing British efforts to discourage the United States from engaging in covert actions to destabilize Soviet-bloc governments in Europe).

[241] Ashley Deeks, Intelligence Communities, Peer Constraints, and the Law, 7 Harv. Nat'l Sec. J. 1, 5 (2015).

[242] Chesterman, supra note 226, at 14, 48–50 (discussing U.S. intelligence sharing with the UN).

[243] Richelson, supra note 226, at 370.

[244] Id. at 395; see also id. (describing Burns-Templer agreement that "allowed the two intelligence communities to pool their resources in 'a full and frank exchange'"); id. (noting that U.S. and Canadian intelligence elements "share diplomatic reporting and threat analysis"); U.S. Dep't of State, Documents Relating to the Exchange of Classified Military Information Between the United States and the United Kingdom (Jan. 27, 1950), https://history.state.gov/historicaldocuments/frus1950v03/d702 [https://perma.cc/KUU7-2-WU7].

meaning. The U.S. efforts to persuade allies not to deploy Huawei's products in their telecommunications systems, for instance, have seen mixed success. Even though the National Security Agency has shared intelligence with allies and partners to underscore the risks of using Huawei tools in their 5G networks, several European states, including the United Kingdom and Germany, "are not convinced that a ban is warranted."[245] Similarly, the United States identified Iran as the author of attacks on two oil tankers in 2019.[246] An expert noted that allies would "want to wait until their intelligence agencies get from the American intelligence community our assessments and forensics . . . before they arrive at their own judgment."[247] This pushback and caution have not caused the United States to change its view, but checks by surrogates will not—and need not—always produce that result.

Beyond checking the quality of U.S. intelligence, at least some foreign allies have challenged the legality of the classified U.S. operations in which they are participating.[248] Most often this will occur when a foreign ally perceives that the United States is violating international law, because that is the body of law that both states may have in common.[249] In the military setting, this might occur during allied detention or targeting operations; in the intelligence setting, it might occur during the conduct of electronic surveillance or rendition operations.[250] The United Kingdom, for instance, repeatedly imposed checks on U.S. detention operations in Iraq, including by conditioning its intelligence sharing on

[245] Christina Zhou & Jason Fang, Why Australia Is Prepared To Ban Huawei from Its 5G Network While the UK and Germany Aren't, ABC News (Mar. 6, 2019), https://www.abc.net.au/news/2019-03-07/why-is-the-uk-seemingly-not-as-worried-about-huawei-as-australia/10866848 [https://perma.cc/VEL9-TCGF]; Rowena Mason, UK Security Chiefs: Huawei Risk in 5G Can Be Contained, Guardian (Feb. 17, 2019), https://www.theguardian.com/technology/2019/feb/17/uk-security-chiefs-huawei-risk-in-5g-can-be-contained [https://perma.cc/N4WA-4MMF].

[246] Robbie Gramer & Lara Seligman, Some U.S. Allies Balk at Blaming Iran for Tanker Attack, Foreign Pol'y (June 14, 2019, 5:03 PM) (quoting expert as noting that "[s]ome U.S. allies may not 'want to be seen as bandwagoning with a U.S. administration that may be seen as a loose cannon on this'").

[247] Id.

[248] See, e.g., Deeks, supra note 241, at 21–23 (describing claims by foreign states that various U.S. intelligence activities were illegal).

[249] For example, Norway's parliamentary oversight committee is required "to help to ensure that the services respect human rights," which includes "an obligation to ensure that the Norwegian intelligence services do not infringe upon these rights." Hernes, supra note 39, at xii.

[250] See Deeks, supra note 241, at 20–23.

humane treatment assurances.[251] In light of German interpretations of international law, Germany refused to provide intelligence to the United States that would enable the United States to use lethal force against German nationals.[252] The United States also has a range of secret bilateral agreements with other states, and those partners have incentives to enforce compliance with those agreements as well.[253]

* * *

This Part demonstrated that the secrecy ecosystem in the United States extends well beyond Congress, the courts, whistleblowers, and leakers. Driven by necessity, the Executive has found itself pressed into relationships with three sets of under-acknowledged secrecy surrogates, each of which has the opportunity in classified settings to contest executive incompetence and illegality and to demand justifications from the Executive for its decisions. This invites several questions: How boldly do these three groups assert themselves in their role as surrogates? What are their incentives to do so? And does the surrogates' pressure on the Executive push in the same direction that the U.S. public would push if it had direct access to these secrets? The next Part considers these questions.

III. THE INCENTIVES OF UNSUNG SECRECY SURROGATES

One persistent problem with relying only on our traditional secrecy surrogates—congressional committees and the courts—is that they sometimes lack robust incentives to serve as checks on the Executive when the latter undertakes classified activities. This Part analyzes what incentives unsung secrecy surrogates have to challenge the Executive's secret intelligence and operations related to cyber, election, and terrorist threats, and how well those incentives align with—and therefore advance—public law values. The Part first argues that the problems that arise from government secrecy reflect the periodic failure of the Executive to conform its actions with public law values. It also argues that actions by unsung secrecy surrogates that counter illegality or flawed analysis, force the Executive to justify its decisions, or challenge the

[251] Id. at 28–29.
[252] Id. at 31–32.
[253] Ashley S. Deeks, A (Qualified) Defense of Secret Agreements, 49 Ariz. St. L.J. 713 (2017).

Executive's classification decisions promote those same public law values. It then explores the incentives of the three unsung secrecy surrogates to test how robust each one's checking function is—or at least has the potential to be. This Part concludes that each of the three surrogates has significant incentives to challenge executive deviations from public law values, at least where the surrogates are sophisticated consumers (and sometimes producers) of intelligence and the national security threat at issue is one that, if unaddressed, will have adverse consequences for the surrogate. This is true even when the surrogates themselves are not driven by public law values in their own acts.

A. Do the Surrogates Advance Public Law Values?

This Article has argued that the three unsung secrecy surrogates are positioned to do something the general public is not: review classified executive information and activities, and check possible abuses of government secrecy in the areas in which those surrogates operate. Part I argued that those abuses fall into four buckets: illegality, incompetence, bad policy decisions, and the ability to avoid justifying policies to actors outside the executive branch.[254] Three of those abuses are relatively policy-neutral. Views about whether something is a bad (or good) policy decision, however, are by definition not policy-neutral. We thus should adopt a healthy skepticism toward having these unsung secrecy surrogates, which owe no democratic or contractual duty to the general public, "check" secret government policy decisions.[255] This Part focuses on the ability of unsung secrecy surrogates to push the government away from committing the three policy-neutral types of abuses, and toward greater compliance with public law values.

The relevant subset of public law values includes (1) legal compliance; (2) competence and rationality; (3) holding government decision makers accountable for the decisions that they have made,[256] including by

[254] See supra Section I.A.

[255] It may be impossible to prevent the unsung surrogates from engaging in policy critiques, however.

[256] In the intelligence setting, one author treats accountability as encompassing "procedures for approval of the gathering, storage, analysis, sharing and dissemination of intelligence, and includes *ex post facto* review of the propriety legality, and effectiveness of the agencies' actions in so doing." Ian Leigh, Accountability and Intelligence Cooperation: Framing the Issue, *in* International Intelligence Cooperation and Accountability, supra note 39, at 4, 6.

demanding justifications for those decisions;[257] and (4) seeking transparency about government decisions where possible.[258] The secrecy surrogates can nudge the Executive toward those public law values by testing whether the Executive appears to be acting in a legal way (or at least not acting in a patently illegal way); whether the Executive appears to be making rational, reasoned decisions based on the secret information it possesses;[259] and whether the Executive is being as transparent as possible, recognizing that some information and acts must necessarily remain secret.[260]

Surrogates themselves need not necessarily embody in their own actions the public law values that we expect from our federal government. For instance, technology corporations are not always transparent in their activities, nor are they legally required or expected to be. What this Part considers instead is whether these actors have incentives to pressure the Executive to act in ways that are consistent with public law values, even if the surrogates' incentives themselves are not fundamentally rooted in the same interests as the U.S. public's. It is a happy coincidence that states, localities, and foreign (democratic) governments themselves face

[257] Deeks, Reason-Giving, supra note 9; Waxman, supra note 15, at 331–32 ("These sorts of deliberative processes within the governmental architecture are especially important when, due to secrecy or other difficulties in public appraisal or scrutiny, electoral politics or public pressures function poorly as a check. In similar ways, *vertical*, inter*level* participation among federal, state, and local governments . . . could subject collaborative policies to mutual review and validation by institutions with overlapping responsibilities but differing political pressures, as each level works to build and maintain the support of the others for its programs.").

[258] Amazon is pursuing a transparency initiative in its own operations. Jay Greene, Amazon's Strategy To Win Over Congressional Critics: Tours of Its Giant Warehouses, Wash. Post (Aug. 21, 2019, 8:00 AM), https://www.washingtonpost.com/technology/-2019/08/21/amazons-strategy-win-over-congressional-critics-tours-its-giant-warehouses/ [https://perma.cc/SDF2-65FW] (quoting Amazon representative as stating, "We encourage policymakers and the general public to tour our facilities because we want them to see all of this for themselves," and noting that a total of 150,000 visitors, including 560 federal, state, and local policymakers and their staffs (plus others) visited 23 Amazon warehouses in 2019).

[259] See Laura A. Dickinson, Regulating the Privatized Security Industry: The Promise of Public/Private Governance, 63 Emory L.J. 417, 435–36 (2013) (arguing that accountability "entails some form of ongoing scrutiny over those carrying out an activity to ensure that those actors fulfill the purposes as specified"); Eichensehr, Public-Private Cybersecurity, supra note 23, at 530 ("[T]he existence of sophisticated private sector attribution capabilities may hold the U.S. government more accountable for accusations it makes against foreign governments as well.").

[260] See Anne Joseph O'Connell, The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World, 94 Calif. L. Rev. 1655, 1657 (2006) (describing transparency and accountability as "core democratic values").

expectations that they will embody some set of public law values, by virtue of being governments representing a population, albeit one different from the U.S. polity as a whole. Further, some scholars have identified ways in which tech companies have begun to comport with public law values in their own actions.[261] Actors that are themselves committed to public law values may be more attractive and effective as secrecy surrogates, because they are more likely to be attuned to whether the Executive practices these values and be more familiar with some of the underlying mechanisms that advance or inhibit such values. It is not a necessary feature of a successful secrecy surrogate, however, that it comply with public law values itself.

B. Surrogates' Incentives

Recall that each of the three unsung secrecy surrogates has something that the Executive wants or needs.[262] As Part II argued, the Executive faces growing pressure to effectively address cyber, election, and terrorism threats; to do so, it increasingly must work with these surrogates, which means that the surrogates have significant room to question executive operations and intelligence without risking access to the same. This also means, though, that these unsung surrogates may not endure forever: unlike Congress and the courts, their relationship with the federal government is opportunistic, springing from the current alignment of security threats. If and as these surrogates become less useful to the federal government, or as the government's core national security priorities shift, their ability to influence executive secrecy will wane. Further, if specific surrogates leak classified information, the Executive will remove those surrogates from the information loop, neutralizing them as surrogates. That said, the unsung surrogates have robust incentives to push the Executive toward public law values.

[261] See Eichensehr, Public-Private Cybersecurity, supra note 23, at 522–23, 534 (discussing cases in which private tech companies have stepped in, "acting in ways that bolster public values," to conduct botnet takedowns and make public cyber attributions). A number of tech companies have adopted policies that incorporate international human rights norms. See Ashley Deeks, A New Tool for Tech Companies: International Law, Lawfare (May 30, 2019, 11:49 AM), https://www.lawfareblog.com/new-tool-tech-companies-international-law [https://perma.cc/YYF5-XJU9].

[262] See generally Brad Smith, Tools and Weapons (2019) (arguing that solutions to cyber threats will not be exclusively governmental or corporate, but both).

1. Technology Companies' Incentives

Public choice theorists assume that the private sector seeks to maximize its own interests in interactions with the government.[263] Nevertheless, when tech companies interact with the Executive in this secrecy ecosystem, their incentives often lead them to push the Executive to adhere to the public law values of accuracy, competence, legality, and—sometimes—transparency. Further, sophisticated tech companies have significant leverage over the government, because they can decline to share unique threat information and have choices about whether and how to respond to the information that the government provides them. This leverage means that tech companies can push harder against what they perceive as executive incompetence and incompletely reasoned decisions than congressional oversight committees or the courts might be willing or able to.

a. Incentives To Demand Accuracy

The primary interest of the public tech companies, as with public companies generally, is to maximize shareholder profits. The fact that tech companies are primarily driven by profit motives means that they need to provide effective products and services. For cybersecurity companies, this means being able to protect their own clients (both corporate and individual) from cyber attacks, help identify attackers, and adjust their clients' cyber defenses after attacks. For software companies such as Microsoft, this means building secure products with few vulnerabilities and updating their systems when vulnerabilities come to light. For both types of companies, accuracy is key: tech companies benefit financially from receiving accurate intelligence and analysis from the Executive because their businesses rely on it. Conversely, companies will suffer if they act on the basis of flawed intelligence. Further, as discussed above, when tech companies inform the government about intrusions or other operations of which the Executive was unaware, they presumably stimulate the intelligence community to collect *more*

[263] Jonathan R. Macey, Public Choice: The Theory of the Firm and the Theory of Market Exchange, 74 Cornell L. Rev. 43 (1988); Jody Freeman, The Private Role in Public Governance, 75 N.Y.U. L. Rev. 543, 562 (2000) (noting that public choice theory suggests that "[p]rivate groups manipulate, pressure, bargain, and bribe to benefit themselves at the expense of others"); Freeman, supra note 21, at 845 ("Even those who resist public choice explanations as too extreme tend to think that private parties play a narrow and mostly rent-seeking role in governance.").

intelligence (in addition to better intelligence).[264] This might offer a subsidiary benefit of improving the intelligence community's technical competence, to the extent that the community has weaknesses.[265]

A secondary interest of tech companies, closely related to the first, is to preserve and enhance their corporate reputation: a positive reputation means more customers, which means higher profits. Like the profit motive, the reputational motive pushes in the direction of accuracy. Providing accurate, effective products attracts more business for those tech companies, as well as favorable media coverage. This reputational interest creates incentives for the companies to push for high quality intelligence from the Executive and to challenge or seek additional context for government information that seems weak or inconsistent with companies' own experiences.[266] Companies can make and have made critical, though unclassified, comments about their experiences with the executive branch; doing so does not reveal classified information but can stimulate the Executive itself—or congressional committees—to take corrective action.[267] These types of critiques also have the potential to shift a secret from being deep to being shallower and can buffer corporate reputations if the companies' critiques signal to the companies' clients that they are the "good guys" in the government-corporate interaction.

b. Incentives To Demand Legality

A company's reputation is also generally bolstered when it acts lawfully and diminished when it acts unlawfully. Those following the

[264] See, e.g., 150 Cong. Rec. S9, 428–29 (daily ed. Sept. 21, 2004) (bipartisan statement favoring competition in intelligence analysis); O'Connell, supra note 260, at 1677 (noting that "if redundancy produces competition, it may yield better outcomes than coordination").

[265] See Johnson, supra note 3, at 62 ("[W]here were the legislative overseers to halt the drift and demand better [information technology] competence in the intelligence community?").

[266] See supra text accompanying notes 185–89 (describing pushback from experienced tech companies about the intelligence they received from the government).

[267] This is the "fire alarm" form of congressional oversight detailed by McCubbins and Schwartz. See Mathew D. McCubbins & Thomas Schwartz, Congressional Oversight Overlooked: Police Patrols Versus Fire Alarms, 28 Am. J. Pol. Sci. 165, 166 (1984). For instance, Rep. Adam Schiff, Chairman of the House Intelligence Committee, recently revealed that he and other top Intelligence Committee officials learned for the first time about Russian attacks on three Senate campaigns when a Microsoft representative discussed those attacks at the Aspen Security Forum. Hannah Knowles, Chairman of House Intelligence Panel Says He First Learned of Russian Attacks on Senate Campaigns at a Security Forum, Wash. Post (July 22, 2019, 11:39 AM), https://www.washingtonpost.com/politics/2019/07/21/schiff-house-intelligence-chair-says-he-first-learned-russian-attacks-senate-campaigns-security-forum/ [https://perma.cc/J3QQ-HZNV].

news are increasingly aware of the interactions between governments and tech companies—including the exchange of information about and responses to hostile cyber operations and election interference. Tech companies fear the taint of being associated in the public mind with perceptions of government illegality, and they might (reasonably) assume that their interactions with the government ultimately will come to light, even if classified. The companies therefore sometimes have challenged the government when asked to undertake operations or share information in a way that pushes the legal envelope.[268]

Recently, a large number of companies have proclaimed that they owe loyalties not only to shareholders, but also to a broader set of stakeholders.[269] Driven in part by an understanding that modern corporations increasingly play an essential role in the health of the country, nearly 200 chief executive officers from companies such as Amazon, Apple, IBM, and Leidos have committed to investing in their employees and supporting the communities in which they operate.[270] This new perspective on the corporate mission may provide another set of incentives for the tech companies to push the government away from legally tenuous activity.

[268] See Barton Gellman & Laura Poitras, U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, Wash. Post (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/V3LD-XL55] (noting that several of the named companies denied granting such access, which some perceived as illegal); cf. Rozenshtein, supra note 22, at 123–24 (noting that "where the law is ambiguous as to what level of process is required, surveillance intermediaries often err on the side of demanding the higher level of process" and that these intermediaries, including Yahoo and Twitter, "regularly push back against surveillance orders"); see Gabriel J.X. Dance & Jennifer Valentino-DeVries, Have a Search Warrant for Data? Google Wants You To Pay, N.Y. Times (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html [https://perma.cc/HV9P-LD25] (discussing Google's decision to charge law enforcement for executing warrants and noting that "privacy experts support such fees as a deterrent to overbroad surveillance").

[269] See, e.g., Bus. Roundtable, Business Roundtable Redefines the Purpose of a Corporation To Promote "An Economy That Serves All Americans" (Aug. 19, 2019), https://www.businessroundtable.org/business-roundtable-redefines-the-purpose-of-a-corporation-to-promote-an-economy-that-serves-all-americans [https://perma.cc/JKZ7-AZ97] (articulating a "modern standard for corporate responsibility" that focuses not just on shareholders but also employees, communities, suppliers, and customers).

[270] Bus. Roundtable, Our Commitment, https://opportunity.businessroundtable.org/ourcommitment [https://perma.cc/3FJK-NJ4B] (last visited Aug. 28, 2020).

c. Incentives To Seek Transparency

Whether for reasons of profit or principle, some tech companies view themselves as advocates for their users' (and potential customers') privacy and security. One way to highlight that they are committed advocates for their customers is to challenge the government in court. In one wave of litigation, tech companies successfully sought to disclose the number of content requests and orders that they had received from the government—information that was classified.[271] In addition, tech and utility companies are pressing the government to declassify cyber threat information to make it more actionable. The companies therefore are using their positions as secrecy surrogates to urge increased transparency about some of the government's cyber and election activities and intelligence.

d. Disincentives To Serve as Robust Secrecy Surrogates

There are several reasons why the companies might not serve as robust surrogates. First, the companies might be disinclined to directly question U.S. intelligence for fear of undercutting their relationships with the intelligence community, even if they disagree with a particular intelligence conclusion. For instance, cooperative companies may receive early warnings from the government about threats that uncooperative companies will not receive.[272] This tentativeness would weaken the strength of the external checks that the companies impose on the Executive. Second, some tech company officials began their careers in the intelligence community and may feel loyalty to or undue confidence in their former colleagues or agencies, notwithstanding their companies' incentives to achieve accuracy. Third, tech companies have financial and reputational motivations that may drive them to act in a way that does not necessarily advance the public interest.[273] For example, a firm might raise questions about or even disregard accurate secret government information

[271] See Eichensehr, Digital Switzerlands, supra note 197, at 677–78 (describing tech companies' litigation seeking the right to publish "aggregate information on the number of [FISA] orders it receives and the number of users covered by the requests"); Complaint at 2, Microsoft v. U.S. Dep't of Just., 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. 2:16-cv-00538) (in which Microsoft argued that a provision of the Electronic Communications Privacy Act violated the First and Fourth Amendments).

[272] Harris, supra note 150.

[273] For a discussion of "public law values" and the extent to which cybersecurity companies pursue those values, see Eichensehr, Public-Private Cybersecurity, supra note 23, at 505, 521.

for reasons driven by business interests, such as where the government concludes that a particular state is responsible for an attack but that state is a client of the technology company. The company's interest in maintaining a reputation for accuracy and integrity might counteract this risk, however. Fourth, a tech company may be uncertain about its own intelligence and analysis, and thus choose to accept government statements as coming from highly resourced and experienced actors. This uncertainty may lessen over time, as companies gain experience with hostile threats, techniques, and procedures.

On the other hand, some companies that have direct, classified *contractual* relationships with the government—and thus might be thought to be very cautious about their willingness to "bite the hand that feeds them"—have started to push back on the underlying U.S. government activity. Perhaps, then, there is a growing willingness among corporations (driven partly by employee demands) to challenge U.S. intelligence and military activities that seem problematic, especially if the companies are not in a direct contractual relationship with the government.[274] Further, the Executive faces growing pressure to share intelligence with companies, and may conclude as a political or security matter that it must sustain that sharing even in the face of critiques from the companies.

In short, in many cases, tech companies' interests will align with the public's interest in executive adherence to public law values such as accuracy, transparency, reason giving, and legality. Both tech companies and the public benefit when the intelligence community collects accurate intelligence and produces solid analyses. The companies enhance their bottom line and their reputation when reliable government information facilitates their ability to make accurate cyber attack attributions and effectively defend their customers against cyber attacks. Indeed, tech companies receive a direct reward for serving as secrecy surrogates that

[274] See Daisuke Wakabayashi & Scott Shane, Google Will Not Renew Pentagon Contract That Upset Employees, N.Y. Times (June 1, 2018), https://www.nytimes.com/2018/06/01/-technology/google-pentagon-project-maven.html [https://perma.cc/SNL9-H94B]; Tony Romm & Drew Harwell, Microsoft Workers Call for Cancelling Military Contract for Technology That Could Turn Warfare into a "Video Game," Wash. Post (Feb. 22, 2019, 5:00 PM), https://www.washingtonpost.com/technology/2019/02/22/microsoft-workers-call-can-celling-military-contract-technology-that-could-turn-warfare-into-video-game/ [https://per-ma.cc/XB2X-2UCT] (noting that Microsoft employees petitioned the CEO to cancel a contract with the U.S. Army for augmented-reality headsets).

demand quality intelligence and press the government for context and justifications.

2. Local Governments' Incentives

As a general matter, relying on local governments as secrecy surrogates to check secret federal government operations may feel far more familiar—and perhaps more comforting—than having tech companies operate as checks. When there are dual sovereigns in place with distinct interests, constituents, and values, Madison reminds us, "a double security arises to the rights of the people."[275] The Supreme Court has noted that the "'constitutionally mandated balance of power' between the States and the Federal Government was adopted by the Framers to ensure the protection of 'our fundamental liberties.'"[276] Matthew Waxman, who has written about what he terms "national security federalism," argues that in the national security area, having federal and local actors share responsibilities can heighten deliberation. Further, he notes that "pushback accounts" of federalism "posit a role for states and local entities in influencing national legal and policy agendas."[277]

In addition to the well-established benefits that some scholars believe that federalism provides, it is reassuring that these secrecy surrogates must adhere to public law values themselves (by virtue of state constitutions and oaths of office, as well as their obligations to comply with federal law). They are habituated to expectations that government officials will act competently, justify their decisions, and favor transparency where possible. Indeed, because local officials are less accustomed to operating within systems that rely heavily on classified information (and because they cannot classify information themselves),

[275] The Federalist No. 51, supra note 32, at 323.

[276] Atascadero State Hosp. v. Scanlon, 473 U.S. 234, 242 (1985) (quoting Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528, 572 (1985)).

[277] Waxman, supra note 15, at 318, 331; see also Bernard Bailyn, The Origins of American Politics 20 (1970) (discussing "counterpoised pressures" that "keep the system stable and healthy"); Deborah Jones Merritt, The Guarantee Clause and State Autonomy: Federalism for a Third Century, 88 Colum. L. Rev. 1, 3–10 (1988) (arguing that federalism provides checks on the central government, as well as greater accessibility, diversity, and increased opportunities for experimentation).

they will be more accustomed to assuming that their decisions and operations will ultimately become public.[278]

Local governments have at least two incentives to check federal government secrecy. First, the governments have strong incentives to ensure the integrity and functionality of their daily operations. Local government officials want to ensure that their constituents' electricity stays on, that their election machines are not tampered with, and that state and city agency websites remain operational. Doing so requires them to accurately assess threats to infrastructure and government operations (including the details of how those targets operate), and to predict the effects of remedial efforts. Officials who fail to do so get voted out of office. Local government efforts to question and confirm the classified cyber and election information that the federal government provides and the operational responses it proposes will push in the direction of accuracy and competency. Doing so will also force the federal government to give reasons for its determinations, which can improve their quality.

Persistent tensions also exist between federal and local governments, including in the counter-terrorism and election spaces.[279] These tensions, which appear to stem both from turf battles and from more abstract conceptions of the proper role of the federal government in elections, may also provide fodder for local governments to challenge the accuracy of secret executive information and advocate for greater transparency about some of that information.[280] In fact, some states initially pushed back

[278] This relative unfamiliarity with classified information might suggest that these individuals are more likely to accidentally leak classified information, though I have found no evidence of this.

[279] Waxman, supra note 15 (discussing such tensions in counter-terrorism); Mark Rockwell, States Resist "Critical Infrastructure" Designation for Election Systems, GCN (Feb. 23, 2017), https://gcn.com/articles/2017/02/23/voting-critical-infrastructure-opposition.aspx [https://perma.cc/996Q-ULSM] ("While some states . . . took DHS up on its offer to provide cybersecurity scans of some of their systems in the wake of attempted hacks into state voter registration systems, others are very wary of letting federal agencies into state-managed facilities for fear of, or the impression of, federal influence or management.").

[280] See Michael S. Greve, Federalism, *in* The Oxford Handbook of the U.S. Constitution 431, 451 (Mark Tushnet, Mark A. Graber & Sanford Levinson eds., 2015) ("[T]he marriage of political calculus and high constitutional argument continuously fuels the federalism debate."); Waxman, supra note 15, at 328–29 (describing tensions between local and federal agents over immigrant interviews in the wake of the September 11 attacks, because local police favored preserving local relationships with Muslim communities rather than rounding up immigrants at the Department of Justice's request); Wines, supra note 17 (quoting state election officials as being puzzled why the federal government insisted that certain threat information remain classified).

against federal government efforts to assist them with their election security because states worried that "their authority was being usurped."[281] When states are unwilling to accept federal assistance, of course, their ability to serve as secrecy surrogates evaporates. The trend now is moving in the other direction, though, with states actively seeking federal assistance to protect elections.[282]

There are reasons to question how robust local governments have been as surrogates to date. Among the three unsung surrogates, local government officials have the least experience with foreign threats and the least sophisticated cyber operators. (This is unlikely to be true for cities such as New York, Los Angeles, and Chicago, however.) This lack of expertise may place officials in a reactive posture, focused on trying to process and implement the information they receive from the Executive rather than challenging the quality of information, its classification level, and the Executive's justifications for its conclusions. If uncertainty exists now, though, it will wane as local governments gain experience with hostile cyber operations and attacks on elections.

Even if states have robust incentives to serve as unsung secrecy surrogates, their role may come with costs. Classified cooperation between federal and local actors may make it harder for the public to assign blame when things go wrong, thus reducing rather than improving accountability for government decision making.[283] In addition, federal actors who handle classified information and operations tend to have more robust internal policies and inter-branch checks than local government officials do, such that the latter may more easily violate individual privacy rights using classified information.[284] There have not

[281] Wines, supra note 17.

[282] Derek B. Johnson, 3 Ways DHS Is Helping States With Election Security, FCW (Jan. 11, 2018), https://fcw.com/articles/2018/01/11/3-ways-dhs-helps-states-voting.aspx [https://perma.cc/FGF9-8LLA] (noting that in 2018, so many states requested federal risk and vulnerability assessments that a backlog formed).

[283] See Waxman, supra note 15, at 330; Rockwell, supra note 279 (quoting the leader of the National Association of Secretaries of State as worrying about whether federal designation of elections systems as "critical infrastructure" would cloud transparency of and accountability for those systems).

[284] Cf. Waxman, supra note 15, at 336 (noting the lack of sophisticated internal controls at the state and local government levels and the lack of expertise among local and state legislatures and courts to conduct rigorous oversight). But see K. Jack Riley, Gregory F. Treverton, Jeremy M. Wilson & Lois M. Davis, State and Local Intelligence in the War on Terrorism 31 (2005) (noting that some cities have independent auditing processes to monitor intelligence activities).

been reports of such violations occurring, however, and on balance the role of local governments as unsung secrecy surrogates seems to be both positive and growing.

3. Foreign Allies' Incentives

Thinking about foreign governments as surrogates for the U.S. polity in relation to secret government operations is admittedly counterintuitive. After all, foreign governments have their own distinct foreign policy and national security interests that will never fully align with those of the United States. They have legal and political duties to their own citizens; sometimes those legal obligations impose higher or lower standards than U.S. law does (though where the United States and its allies share international legal obligations, the standards may be comparable). But they often have incentives to prod the Executive to adhere to its own public law values, and they have leverage over the Executive: the ability to share or withhold intelligence or to grant or withhold consent to use their territory, airspace, or cyber infrastructure for counter-terrorism or counter-cyber operations. When foreign allies themselves take seriously public law values, including the need to ensure that governments adhere to the law and justify their decisions, they can serve as useful secrecy surrogates.

a. Incentives To Demand Accuracy

As with the needs of tech companies and local governments, the operational needs of foreign allies will generally lead them to favor (if not demand) accuracy and competence in their dealings with U.S. intelligence officials. Like local U.S. governments, the governments of NATO allies want and need to conduct effective counter-terrorism operations and halt election interference and hostile cyber operations against targets in their countries. This means that they have strong incentives to question U.S. intelligence, analysis, and conclusions before accepting them and incorporating them in their own operations. News reports surrounding the U.S. conclusions about the attacks on oil tankers in 2019 and about the threat posed by Huawei indicate that foreign allies are engaged in just such questioning.[285] Even if the United States concludes that its

[285] Betsy Swan & Adam Rawnsley, Trump Admin Inflated Iran Intel, U.S. Officials Say, Daily Beast (May 8, 2019), https://www.thedailybeast.com/trump-administration-inflated-iran-intelligence-us-officials-say [https://perma.cc/98K6-JAZA] ("[T]here is not a consensus

intelligence is correct, it is healthy for trusted outsiders to question that intelligence without leaking it.

b. Incentives To Demand Legality

I have argued elsewhere that foreign intelligence services can and do engage with the U.S. intelligence community about the legality of the latter's actions, and in some cases press U.S. intelligence officials towards stricter compliance with international law.[286] Foreign allies are concerned about leaks and worry about perceptions of cooperating with the United States on national security issues on which the United States has tended to interpret international legal authorities permissively.[287] Further, foreign allies have faced a raft of litigation over such cooperation in the post-9/11 era.[288] Because "it has become increasingly common for governments to take executive decisions on the basis of information received from foreign services,"[289] the allies receiving such information from the United States will want to ensure its accuracy and legality in case the allies' overseers (parliaments, domestic courts, or the European Court of Human Rights) end up reviewing the case. A state also may be worried about operating jointly with the United States when the United States is engaging in international law violations out of concern that those wrongful acts may also be attributed to the first state under international law principles of state responsibility.[290]

As a result of leaks and litigation, these foreign actors "come to their liaison relationships with law on their mind" and are positioned, "as a matter of choice or necessity, to constrain" their U.S. peers.[291] This type of engagement, which tends to focus on international legal compliance,

in intelligence and military circles on whether the administration's interpretation, used to justify the deployment of an addition [sic] U.S. aircraft carrier and Air Force bomber task force to the Gulf, was accurate. The interpretation of intelligence, particularly on Iran, can often provoke disagreements within the national security bureaucracy.").

[286] Deeks, supra note 241, at 28–34.

[287] Id. at 11.

[288] Id. at 14–15.

[289] Wills & Born, supra note 225, at 281.

[290] See, e.g., Martin Scheinin & Mathias Vermeulen, International Law: Human Rights Law and State Responsibility, *in* International Intelligence Cooperation and Accountability, supra note 39, at 258, 260–65 (discussing Draft Articles provisions on aiding and assisting in a wrongful act and obligations not to recognize or assist in unlawful situations).

[291] Deeks, supra note 241, at 23.

complements the engagement by the two other unsung secrecy surrogates, whose concerns about legality will emphasize U.S. domestic law.

c. Incentives To Seek Transparency

Unlike tech companies and local governments, foreign allies have few incentives to press the U.S. Executive to declassify information. In a handful of cases, the United States and its allies seem to have agreed collectively to make public attributions about cyber attacks, but it is unclear which state took the lead on pressing for transparency.[292] It is therefore useful that other unsung secrecy surrogates have slightly different incentives that provide overlapping but not identical friction with the Executive.

d. Incentives Against Robust Checking

Foreign allies face certain limitations on serving as robust checks on the Executive. Presumably an ally's foremost concern is that it will lose access to U.S. intelligence and cooperation if the United States begins to view it as a difficult partner. A second concern is that some allies may themselves have insufficient intelligence capabilities to be able to detect flaws in U.S. analysis or conclusions—though even these types of allies can ask probing questions about the intelligence on its face. A third concern is that a foreign ally might be aware that the United States has reached a flawed conclusion about, say, a terrorist cell, but might choose not to challenge that intelligence because it believes that the faulty intelligence will lead the United States to detain someone disfavored by the ally's government. In any given case, one or more of these incentives might arise and override the benefits of accuracy and legality, but the pressures to demand accuracy and legality as a general matter seem likely to prevail.

[292] See Catalin Cimpanu, UK Says It Warned 16 NATO Allies of Russian Hacking Activities, ZDNet (May 23, 2019, 11:40 AM), https://www.zdnet.com/article/uk-says-it-warned-16-nato-allies-of-russian-hacking-activities/ [https://perma.cc/23JL-S3E4] (describing how the UK and Netherlands are moving to a "name-and-shame" approach when dealing with cyber attacks).

* * *

The three groups of unsung secrecy surrogates that are this Article's focus have a range of incentives to steer the Executive toward public law values and away from some of the perversities that government secrecy can conceal. They interact with the Executive on different—though overlapping—issues, and each surrogate has slightly different incentives to check the Executive. Because the Executive needs the surrogates' cooperation, and the success of the Executive is intertwined with the surrogates' successes, the Executive has a persistent incentive to reveal at least some classified information and accept some level of challenge to its shared operations, particularly when the surrogates are sophisticated players. In fact, these actors may be *better* positioned to serve as surrogates than congressional committees and the courts because the unsung surrogates have an operational need for—and therefore strong incentives to seek—accurate intelligence.

IV. STRENGTHENING THE SECRECY SYNOPTICON?

Part III demonstrated that each unsung secrecy surrogate provides checks on government secrecy that advance some public law values. As these unsung surrogates join the traditional secrecy surrogates, the system begins to look like what Jack Goldsmith described as a synopticon: a collection of "watchers" who gaze on a single actor.[293] Goldsmith described a presidential synopticon that intently focused its attention on the executive branch's conduct in war.[294] Today's national security threats have—quite inadvertently—moved us closer to a "secrecy synopticon." In a secrecy synopticon, a variety of actors observe a range of secret government information and decisions and are positioned to "promote[] responsible executive action"[295] without revealing the secrets themselves. The fact that each surrogate—whether traditional or unsung—has overlapping but non-identical incentives is a feature, not a bug: their diversity strengthens the secrecy synopticon.

Consider three ways in which the surrogates may interact with each other to enhance the existing secrecy synopticon. First, in situations in

[293] Goldsmith, supra note 29, at 205–06.
[294] Id. at 207.
[295] Id.

which states, cities, or foreign allies hire private cybersecurity firms, we might see particularly strong checks on the Executive because two sets of unsung surrogates are combining their expertise to evaluate the quality, sufficiency, and legality of executive intelligence.[296] Second, Congress, acting in its traditional surrogate role, can draw on the unsung surrogates' exposure to executive operations to increase its own visibility into executive cyber, election, and counter-terrorism operations. Third, the persistent and inevitable role of leakers in the secrecy ecosystem increases the incentives of tech companies to challenge secret executive acts that are of questionable legality, out of fear that their cooperation with the government on legally controversial classified programs will come to light through a leak.

This Part first identifies and addresses potential critiques of characterizing the current system as an effective secrecy synopticon. It then offers some prescriptions for ensuring that the unsung secrecy surrogates can sustain their willingness and ability to check erroneous, insufficiently justified, or illegal executive policies or operations.

A. Does the Secrecy Synopticon Really Work?

Part III argued that significant benefits flow from the operation of the unsung secrecy surrogates. Nevertheless, one can imagine several challenges to the argument that unsung secrecy surrogates can improve and are improving secret executive activities. First, we might worry that the constraints they impose are stochastic.[297] As such, secrecy surrogates will choose to check government secrecy in unpredictable and possibly random ways, so their effectiveness will also be unpredictable. Further, the Executive still controls which secrets it shares with the surrogates; it

[296] See FireEye, State and Local Government Cyber Security, https://www.fireeye.com/solutions/government/state-and-local-governments-and-education-services.html [https://perma.cc/J2B5-WYD9] (last visited Aug. 26, 2020) (discussing the company's role in assisting state and local governments); FireEye, Federal Government Cyber Security, https://www.fireeye.com/solutions/government/federal-government.html [https://perma.cc/X2FG-9FHS] (last visited Aug. 26, 2020) (noting that the company has a partnership with Singapore's Cyber Security Agency and exchanges "knowledge and expertise" with the European Crime Center).

[297] See Katyal, supra note 59, at 1001–02 (objecting to Jack Goldsmith's approbation of ex post checks on the Executive because "these checks are unpredictable by their nature and risk being overreactive," and "[u]ltimately, there is no way to know if, how, or when Goldsmith's different, newfangled checks will operate"). Katyal also notes that it matters which actors provide checks; courts can provide decades-long constraints, while other checks may be less durable. Id.

could choose to withhold wide swaths of analysis without anyone being the wiser. The reverse is also true: the surrogates decide how much to engage with the Executive in the classified space. In theory, they could reduce their counter-terrorism, cyber, and election cooperation with the Executive and thus cede their role as surrogates.[298] In light of threat trends; increased public pressure on the Executive, U.S. states, and foreign allies to effectively address cyber and election threats; and the profit motives of tech companies, however, it seems unlikely that cooperation among the Executive and the unsung surrogates will play out this way. As long as the unsung surrogates feel pressure to protect their constituents or customers from cyber, election, and terrorism threats, and as long as those constituents or customers view legal compliance as a public law value, we can expect the surrogates to provide regular pressure on the Executive.

Another problem with relying on a stochastic synopticon to check the Executive is that it may distract us from trying to improve the internal processes that allow the Executive to abuse secrecy.[299] Katyal might frame the unsung surrogates as quality control operators on a factory line: they may spot certain defective products, but they will do nothing ex ante to improve the underlying system that produces those defects. However, unlike mechanized factory lines that produce inanimate objects, the Executive is aware that its secret "products" will face scrutiny by the surrogates, at least in some cases, and it will generally take steps in advance to anticipate critiques, even if it is uncertain in any particular case whether the surrogates will challenge its activities.[300] Further, even if Katyal is correct that it would be better to improve the Executive's internal procedures directly, this has proven to be a Herculean task.[301]

Second, some will argue that we should be suspicious about relying on tech companies as surrogates. Giving companies access to classified

[298] See Bruce Schneier, Data and Goliath: The Hidden Battles To Collect Your Data and Control Your World 209 (2015) (discussing temporary nature of alignment of interests between tech companies and government); Eichensehr, Public-Private Cybersecurity, supra note 23, at 535 (same); Eichensehr, Digital Switzerlands, supra note 197, at 727–30 (discussing "backsliding" by companies).

[299] See Katyal, supra note 59, at 991 ("Goldsmith fails to account for the value served by good process. . . . [T]he path by which the Executive is constrained matters, because it will significantly affect the substantive quality and sustainability of that end result.").

[300] See Ashley S. Deeks, The Observer Effect: National Security Litigation, Executive Policy Changes, and Judicial Deference, 82 Fordham L. Rev. 827, 833–34 (2013).

[301] See Sagar, supra note 7, at 188–89 (concluding that it is very difficult to improve executive secrecy processes).

material allows them to use that material to bolster their profits or gain a competitive advantage.[302] The fact that the Executive is empowering some set of already-powerful private actors by sharing government secrets with them may compound the current perception that excessive government secrecy compromises participatory democracy. While this perception may be both real and problematic, Parts II and III illustrated why tech companies may be one of the better tools the public has in its toolkit to check an even more powerful actor: the national security executive.[303]

Others will argue that companies previously assisted the U.S. government or foreign governments on national security projects in ways that undercut civil liberties, and that we should therefore be skeptical that they will act as our surrogates to check the government.[304] In addition, even if the tech company surrogates are not acting as government contractors when they interact with the Executive on attribution and cyber defense issues, some of these surrogates do have separate contracts with the Executive and may be inclined to pull their punches to preserve those contractual relationships. There is another story to tell here, however, one that emphasizes the companies' interest in being seen as an advocate for their customers' interests and in disassociating themselves from executive

[302] See Shorrock, supra note 182 ("[T]he cyberintelligence-industrial complex is qualitatively different from—and more dangerous than—the military-industrial complex . . . . This is because its implications for democracy, inequality, and secrecy are far more insidious. . . . By retaining their security clearances, many of its members have access to the most highly guarded intelligence, which they use to the benefit of their corporate and government clients."); Edward Lucas, The Spycraft Revolution, Foreign Pol'y (Apr. 27, 2019), https://foreignpolicy.com/2019/04/27/the-spycraft-revolution-espionage-technology/ [https://perma.cc/6FP6-3FMS] ("[P]ublic tolerance is waning as knowledge, trade-craft, and contacts gained at taxpayer expense are used for self-enrichment in retirement."). On the other hand, as Secretary of War Henry Stimson argued in 1940, "If you are going to try to go to war, or to prepare for war, in a capitalist country, you have got to let business make money out of the process or business won't work." Allan M. Winkler, World War II, *in* The Concise Princeton Encyclopedia of American Political History 1009, 1011 (Michael Kazin ed., 2011).

[303] See Eichensehr, Digital Switzerlands, supra note 197, at 715 ("[H]aving two powerful regulators, rather than only one, can sometimes strengthen individuals' freedom, liberty, and security because often it takes a powerful regulator to challenge and check another powerful regulator.").

[304] See Harris, supra note 110, at 114 (describing cybersecurity companies as "being bagmen for governments"); Jon D. Michaels, All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror, 96 Calif. L. Rev. 901, 901–02 (2008); Google's Project Dragonfly "Terminated" in China, BBC (July 17, 2019), https://www.bbc.com/news/-technology-49015516 [https://perma.cc/UP9T-XUSQ] (discussing Google's cooperation with China to develop a censored search engine).

branch illegality. The proliferation of leaks, which can reveal confidential relationships between the government and tech companies, makes these corporate interests particularly sharp. The challenge will be to sustain a relationship between the tech companies and government that is healthily skeptical. The next Section considers ways to do so.

A third concern about adding new players to the secrecy synopticon is that it will increase the risk of leaks and the number of targets that adversaries could hack. This concern is real. Although the Executive has created a formalized process by which to provide security clearances, has threatened tech company officials if they leak information, and could prosecute individuals who violate their non-disclosure agreements, it is true that any act that disperses secrets more widely makes it more likely that the secrets will leak. There have been no high-profile stories of leaks by the unsung secrecy surrogates, nor have there been reports on adversarial efforts to hack the surrogates for the purpose of gaining access to executive data or plans. Nevertheless, the possibility remains.

Finally, one might question the strength of a "secrecy synopticon" that has a relatively narrow remit. Many of the secrecy surrogates have access to only a narrow sliver of executive intelligence and programs. The Executive will continue to conceal wide swaths of U.S. military and intelligence operations—covert operations, highly classified collection techniques, and advanced technologies—from these unsung secrecy surrogates. This objection is valid: as with every other corrective in the government secrecy space, the roles of the unsung secrecy surrogates and the "secrecy synopticon" are patchwork and therefore imperfect. The first best system would be an angelic Executive that is truly committed to adhering strictly to legal frameworks, maximizing competent collection and analysis, and welcoming accountability and oversight. The second best system is a form of the grand bargain struck in the 1970s, supplemented by the growing secrecy synopticon, in which different actors with different interests and perspectives gain access to different parts of the secrecy ecosystem and check the secret executive in a panoply of ways.[305]

[305] Recall that other actors participate in the secrecy synopticon as well, including the PCLOB, inspectors general, and the President's Defense Policy Board and Intelligence Advisory Board.

B. Should We Strengthen the Synopticon?

On balance, the turn to unsung secrecy surrogates and the expansion of the secrecy synopticon appears to be a positive one. This development is contingent on preserving a posture of moderate but not paralyzing friction between the Executive and the surrogates, however. There are several steps we could take to sustain this moderate friction while enhancing the surrogates' efficacy. First, Congress could require that the Executive provide the surrogates with access to more and different forms of intelligence and analysis in the cyber, elections, and counter-terrorism arenas. Second, Congress could ensure that the technology company and local government surrogates perceive themselves to be serving as surrogates for the U.S. polity and that they take that role seriously. Third, Congress and state legislatures should view the unsung surrogates as a new avenue through which to seek information about executive activities.

1. Widening Access to Secrets

The most straightforward step that Congress could take to enhance the synopticon would be to increase the unsung surrogates' access to classified threat information and operations related to cyber, elections, and terrorism. Congress has already taken steps in this direction with the Cyber Information Sharing Act, which facilitates and encourages the sharing of "cyber threat indicators" among federal and non-federal actors, including states and localities and the private sector.[306] But some agencies have been delinquent in implementing CISA.[307] Congress should demand that agencies fully implement the statute and insist on increased classified information sharing, so that the surrogates understand the context in which the threats arise and are able to operationalize—and challenge—that intelligence more easily. Further, Congress could expand the CISA approach into the election arena, requiring that the Executive share more detailed classified threat information with state and local election officials, as well as with tech companies that help protect those elections.

[306] See supra text accompanying notes 163–64.

[307] See Off. of Inspector Gen., Dep't of Def., Rep. No. DODIG-2019-016, DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements (Nov. 8, 2018), https://www.dodig.mil/reports.html/Article/1688703/dod-actions-to-implement-the-cyber-security-information-sharing-act-of-2015-requ/ [https://perma.cc/K9F4-6UPT] (critiquing the Defense Department's implementation of CISA as of 2018).

The idea of increasing intelligence sharing in these areas is not novel. Several task forces and scholars have proposed ways to streamline and enhance existing intelligence sharing between the federal government and states, localities, and companies.[308] The goal of most of these proposals is to further the country's overall ability to address national security threats, but these proposals would, if implemented, have the subsidiary benefit of enhancing the opportunity for the secrecy surrogates to advance public law values in ways discussed in Parts II and III. Even if there are costs to widening the synopticon's aperture, increasing the sharing of classified information ultimately may be imperative to protect U.S. infrastructure and the economy.

Robert Knake, for example, has urged the government to provide critical infrastructure companies, which "have been recognized as facing a severe threat from our Nation's adversaries," with more classified information under the Obama Administration executive order intended to facilitate cybersecurity information sharing with entities controlling critical infrastructure.[309] Because the Executive has been slow to do so on its own initiative, Congress could accelerate this process by statute and ensure that tech companies and local governments are included in the process. Knake also recommends providing the critical infrastructure companies with access to a classified computer network, rather than relying on the slower processes of declassification or classified briefings. His model is the Defense Industrial Base Network, an online system through which the Defense Department shares classified information on cyber threats, mitigation, and remediation strategies with its

[308] See, e.g., The President's Nat'l Infrastructure Advisory Council, Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure 3–4 (2017), https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf [https://perma.cc/M2ML-JZFC] (calling for improvements such as streamlining the security clearance process for owners of critical cyber assets and rapid declassification of cyber threat information).

[309] Cyber Threat Information Sharing (statement of Robert K. Knake, Senior Fellow, Council on Foreign Relations), supra note 184, at 11; see also Exec. Order No. 13,636, § 4(b), 78 Fed. Reg. 11,739 (Feb. 12, 2013) ("The Secretary and the Attorney General, in coordination with the Director of National Intelligence, shall establish a process that rapidly disseminates the reports produced pursuant to section 4(a) of this order to the targeted entity. Such process shall also, consistent with the need to protect national security information, include the dissemination of classified reports to critical infrastructure entities authorized to receive them.").

contractors.[310] Further, if the Joint Terrorism Task Forces have been effective, it might be possible to use the intelligence sharing systems created therein to share cyber and election intelligence with state and local officials.

The Cyberspace Solarium Commission, a body created by Congress "to develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences," is the most comprehensive effort to date to address the challenges of cyber information sharing among federal, local, and private sector actors.[311] The Commission proposed that Congress "establish a 'Joint Collaborative Environment,' a common, cloud-based environment in which the federal government's unclassified and classified cyber threat information, malware forensics, and network data from monitoring programs are made commonly available for query and analysis—to the greatest extent possible."[312] The proposal addresses the fact that the government's and private sector's information about cyber threats are not well-integrated. If such a program could "make real the promise of a 'whole-of-government' and public-private approach to cybersecurity,"[313] it also would expand the opportunity for private sector companies to serve as secrecy surrogates.

The Executive and Congress might also re-evaluate *which types* of officials the Executive shares information with. Although it is difficult to ascertain the specific types of officials with whom the Executive currently shares threat information, it may be the case that the Executive tends to share information with individuals who are experts in cyber technology. However, C-suite executives, risk-assessment officers, and the political leadership of the local governments are best suited to put a particular threat in a larger commercial and geo-political context and to evaluate the overall risk for the company or local government. Therefore, just as David Pozen has identified the advantages of broadening the types of executive branch officials who are aware of a secret,[314] so too might there be

[310] DIBNet Portal, Dep't of Def., https://dibnet.dod.mil/portal/intranet/ [https://perma.cc/-2N7C-HU69] (last visited Aug. 26, 2020); Cyber Threat Information Sharing (statement of Robert K. Knake, Senior Fellow, Council on Foreign Relations), supra note 184, at 11.

[311] About, U.S. Cyberspace Solarium Comm'n, https://www.solarium.gov/about [https://perma.cc/Q6GM-4FZW] (last visited Aug. 26, 2020).

[312] U.S. Cyberspace Solarium Comm'n, Final Report 102 (2020), https://drive.google.com/-file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [https://perma.cc/5PYG-SWZG].

[313] Id.

[314] Pozen, supra note 5, at 333.

advantages to giving different types of tech company or local government officials access to the secret information and operations.

There presumably are a few reasons why the intelligence community has shared only limited classified information with companies and localities to date. First, as discussed *supra*, sharing secrets with more actors expands the surface area of those secrets, so that there are more avenues for other actors, including foreign governments, to steal them. Second, sharing these secrets increases the chance of leaks, particularly where the surrogate's employees object to the underlying act that the government expects the company to take or question the quality of the intelligence that the government shared. Third, the clearance process is both expensive and time-consuming, and the government generally requires corporate and local officials to obtain some type of security clearance before receiving sensitive threat information. Congress would thus have to be willing to provide sufficient funding to support the clearance process for greater numbers of individuals in tech companies and local governments, and should be willing to increase funding to offices in the Justice Department that investigate leaks, if that proves necessary. If leaks do not increase and the cooperation produces operational results, executive officials who today staunchly resist any secret sharing might begin to soften their views against such sharing.

2. Offering Carrots and Sticks

Congress may also need to offer carrots and sticks to the surrogates to help sustain a healthy balance between the surrogates and the Executive. Some news reports suggest that companies have been slow to join programs such as CISA's Automated Indicator Sharing Program, which provides declassified threat indicators.[315] Companies complain that the notices are "late and lack important context."[316] As the Executive improves the access to and the quality of the intelligence it shares, companies may naturally gravitate toward these briefings, but Congress might also consider indemnifying those actors who receive briefings and act reasonably on the intelligence received, even if harm incidentally

[315] See Cyber Threat Information Sharing (statement of Rep. Langevin), supra note 184, at 7 (noting that "[b]arely more than 100 companies have elected to join the [Automated Indicator Sharing Program under CISA, which provides declassified threat indicators], a level of participation that is . . . unacceptable").

[316] Id. at 4.

results.[317] As a stick, Congress might impose civil penalties on those tech companies that refuse to receive threat briefings.

Congress could choose to be more aggressive, mandating by statute that the tech companies (or other companies that own critical infrastructure) not only accept threat intelligence from the government but also share threat information with the government when the threat surpasses a certain level of seriousness.[318] One model here is the Bank Secrecy Act ("BSA"), which requires financial institutions to help U.S. government agencies detect and prevent money laundering.[319] In particular, the BSA requires financial institutions to submit suspicious activity reports ("SARs") to regulators within thirty days of detecting criminal violations or transactions that appear to involve money laundering or terrorist financing, or are not the "types of transactions a particular customer would normally be expected to engage in."[320] The BSA also provides a safe harbor for banks when they submit SARs, and it requires that the SARs remain confidential.[321] Translating this to the cyber setting, Congress could mandate that tech companies (as well as other companies such as banks and utilities) submit confidential SARs immediately after detecting serious cyber attacks, while providing a safe harbor against civil litigation.

Providing carrots and sticks to local governments to ensure that they sustain their position as secrecy surrogates is a harder political challenge,

[317] Congress could, for instance, amend CISA, which already provides liability protection for cyber threat sharing by private companies with other companies, with non-federal entities such as the Information Sharing and Analysis Organizations, and with federal entities such as DHS and law enforcement agencies. See Cybersecurity Information Sharing Act—Frequently Asked Questions 2–3, https://www.us-cert.gov/sites/default/files/ais_files/CISA_FAQs.pdf [https://perma.cc/NB73-SLUW] (last visited Oct. 12, 2020).

[318] The Cyberspace Solarium Commission recommended something similar. Its Final Report urges Congress to pass a "national cyber incident reporting law." U.S. Cyberspace Solarium Comm'n, supra note 312, at 103–04; see also id. at 97 ("Congress should codify into law the concept of 'systemically important critical infrastructure,' whereby entities responsible for systemically critical systems and assets are granted special assistance from the U.S. government and shoulder additional security and information-sharing requirements befitting their unique status and importance.").

[319] Bank Secrecy Act, 31 U.S.C. §§ 5311–32 (2018).

[320] Customer Due Diligence—Overview, FFIEC BSA/AML Examination Manual 4 (2018), https://www.ffiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf [https://perma.cc/FRJ7-ZLM3].

[321] See Suspicious Activity Reporting—Overview, FFIEC BSA/AML Examination Manual 73 (2015), https://bsaaml.ffiec.gov/docs/manual/06_AssessingComplianceWithBSARegulatoryRequirements/04.pdf [https://perma.cc/35RZ-7GQM].

particularly when it comes to elections. In light of the federalism sensitivities that surround election operations, congressional efforts to directly build carrots and sticks into election-related legislation may be impossible. A better approach might be to rely on citizens, think tanks, and other actors who appreciate the benefits of state-run elections but who recognize the advantages of the federal government's intelligence to urge state and local officials to view themselves as secrecy surrogates. Moving beyond elections, the constituents for whom the localities serve most directly as secrecy surrogates should communicate that they view the localities as an important check on the quality of federal government operations and intelligence in the cybersecurity and counter-terrorism fields as well.

3. Increasing Interactions with Congress

Unsung secrecy surrogates provide a distinct avenue by which congressional committees and staffers can triangulate their collection of information about secret government operations. That is, congressional committees can convene hearings and request briefings from tech companies and local government officials (in both public and non-public settings). The idea is not that the unsung surrogates will share classified information with Congress (though in some settings that might be appropriate), but rather that Congress can glean information about and evaluate the Executive's national security activities by engaging in conversations with and receiving testimony from these surrogates. Particularly where the Executive has not been forthcoming with Congress, congressional committees and their staffers may be able to extract additional information from tech companies and local officials, either in hearings or in more informal interactions. Tech companies in particular might choose to share information about their role as secrecy surrogates as a way to curry favor with a Congress that has sometimes been hostile toward their interests.[322] State legislatures, too, can seek unclassified information about the activities of the tech companies and the state and local officials involved in cyber, election, and counter-terrorism operations, thus raising the profile of those interactions for the general public.

[322] See Ryan Tracy, Tech Giants Draw Fire in Congress, Wall St. J. (July 16, 2019), https://www.wsj.com/articles/congress-puts-big-tech-in-crosshairs-11563311754 [https://perma.cc/2A55-NLVK].

CONCLUSION

This Article argued that we find ourselves presented with a new set of tools that can reduce some of the persistent problems of government secrecy. Although not democratically accountable to the national polity, these unsung secrecy surrogates have incentives to challenge the Executive in ways that push it toward greater compliance with public law values such as accuracy, legality, and transparency. When considered in combination with our traditional secrecy surrogates (Congress, the courts, leakers, and whistleblowers), the unsung surrogates allow us to rely less heavily on the aspirational ideals of faithful agency and self-discipline in the Executive in trying to minimize the problems with government secrecy. Further, a study of these unsung surrogates reinforces the idea that a key way to check abuses of government secrecy is to align the self-interest of those who have access to secrets with public law values.[323]

Moving forward, the existence of secrecy surrogates opens up a range of questions about how to conceive of government secrecy itself. We usually think of "secrets" and "intelligence" as pieces of highly sensitive information in the hands of federal executive actors. However, this study of secrecy surrogacy highlights that reams of information critical to U.S. national security are now uncovered and possessed by actors outside of the Executive who lack classification authority. Secrecy is a construct, not a pre-ordained designation, and the fact that critical cyber threat, election, and terrorism information is being generated and analyzed by non-traditional actors raises important questions about whether our secrecy constructs should be updated in this new era.

[323] See, e.g., Steven Aftergood, An Inquiry into the Dynamics of Government Secrecy, 48 Harv. C.R.-C.L. L. Rev. 511, 516 (2013) (discussing how "entrenched secrecy policies can be reversed when bureaucratic self-interest dictates such a reversal").