A RULE OF LENITY FOR NATIONAL SECURITY SURVEILLANCE LAW

Orin S. Kerr[*]

ABSTRACT

This Essay argues that Congress should adopt a rule of narrow construction of the national security surveillance statutes. Under this interpretive rule, which the Essay calls a "rule of lenity," ambiguity in the powers granted to the executive branch in the sections of the United States Code on national security surveillance should trigger a narrow judicial interpretation in favor of the individual and against the State. A rule of lenity would push Congress to be the primary decision maker to balance privacy and security when technology changes, limiting the rulemaking power of the secret Foreign Intelligence Surveillance Court. A rule of lenity would help restore the power over national security surveillance law to where it belongs: The People.

INTRODUCTION

IN the summer of 2013, Edward Snowden began an astonishing series of national security leaks that shed new light on the classified work of the Foreign Intelligence Surveillance Court ("FISC").[1] Created in 1978, the FISC was designed to introduce a judicial role into the U.S. regime of foreign intelligence surveillance.[2] The Snowden leaks revealed that the FISC operated differently than outsiders had assumed. Although the FISC had been created primarily as a court to review warrant applications, it had morphed into a regulatory body that issued long opinions

[*] Fred C. Stevenson Research Professor, The George Washington University Law School. Thanks to David Kris, Barry Friedman, Abbe Gluck, Nicholas Quinn Rosenkranz, and Michael Levy for comments on a prior draft, and to Steve Vladeck and members of the Privacy and Civil Liberties Oversight Board for helpful discussions of this proposal.

[1] See Luke Harding, The Snowden Files: The Inside Story of the World's Most Wanted Man 5, 9–11 (2014). The disclosures began on June 5, 2013. See Dustin Volz, Everything We Learned from Edward Snowden in 2013, Nat'l J. (Dec. 31, 2013), http://www.nationaljournal.com/defense/everything-we-learned-from-edward-snowden-in-2013-20131231.

[2] For a history and overview of the Foreign Intelligence Surveillance Act ("FISA"), see 1 David S. Kris & J. Douglas Wilson, National Security & Prosecutions 2d chs. 1–4 (2012).

secretly approving surveillance programs that Congress had never considered—and likely would not have approved.[3]

In the wake of the Snowden disclosures, many proposals have been introduced to improve the FISC. Several proposals would create a "special advocate" for the FISC who could appear before the court and argue against the government, fostering an adversarial process that would facilitate better decision making.[4] Others have proposed that the FISC's opinions should be regularly published; still others, that its decisions should be more readily appealed.[5] All of these reform proposals share a common goal: They aim to make the FISC more like a regular lawmaking court. They try to improve the FISC by blending the characteristics of an ex parte court that merely reviews court order applications with those of a traditional adversarial lawmaking court. By helping the FISC act more like an adversarial lawmaking court, the thinking runs, the reforms can improve the decision making of the FISC and ensure more reliable interpretations of the foreign intelligence surveillance laws.

This Essay will take a different approach. It will argue that Congress should go in the opposite direction: Instead of helping the FISC act more like a regular lawmaking court, Congress should improve the surveillance laws by making sure the FISC will not act as a lawmaking court. Congress should enact an interpretive rule directing that government powers granted under the Foreign Intelligence Surveillance Act ("FISA") should be narrowly construed. I will call this rule of narrow construction a "rule of lenity," borrowing a term often used to advocate a narrow interpretation of criminal statutes. When the government's power under existing law is ambiguous, the FISC should adopt the narrower construction that favors the individual instead of the State. If the executive wants new surveillance powers, it should go to Congress for those powers instead of to the courts. Within constitutional boundaries, the power to define national security law will rest with the elected branches, and in turn, with the people.

Adopting a rule of narrow interpretation for national security surveillance law would have three important benefits.[6] First, it would promote democratic accountability and transparency. It would limit the decision-making authority of the secret FISC and give that power to the open and

[3] See infra Part II.
[4] See infra Section II.C.
[5] See infra Section II.C.
[6] See infra Section III.C.

public legislature. It would enable a feedback loop that allows the public to control the scope of government powers through the elected branches. Second, a narrow interpretive approach would shift power to the branch of government best suited to balance privacy and security in changing technologies. FISC judges are poorly suited to choose surveillance rules, as they are merely trial judges acting in secret without the benefit of adversarial briefing and public commentary. Congress is much better suited to draw the appropriate lines of power. Congress can draw on experts, legislate comprehensively, and account for the latest technological developments.

Finally, a rule of narrow interpretation would avoid the difficult conceptual and constitutional issues raised by existing proposals that try to make the FISC more like a regular court.[7] The hybrid model of an adversarial and an ex parte court envisioned by reformers raises difficult policy choices and creates substantial constitutional concerns under both Article III and the Appointments Clause.[8] Adopting a rule of lenity would avoid those difficulties. Of course, adopting a rule of interpretation would not be a panacea. It would be helpful only to the extent courts follow it, and it would facilitate process rather than guarantee any particular surveillance rule. At the same time, a rule of lenity would provide a simple mechanism to encourage more transparent and effective surveillance laws. It would not solve everything. But it is an easy first step.

This Essay will proceed in three parts. Part I will explain the basic dynamic of ex parte regulation in surveillance law, as well as the special challenges of using that model to regulate national security surveillance law. Part II will explain how Edward Snowden's disclosures have revealed the FISC's failed efforts to act as a lawmaking court in its ex parte role. It will then survey proposals to amend the FISC to bolster its lawmaking function. Part III will propose that Congress should instead adopt a rule of lenity. It will explain the benefits of a rule of lenity, and it will consider how the rule would act in practice to further more accountable and balanced surveillance laws.

[7] See infra Section III.C.
[8] See infra Section III.C.

I. EX PARTE REGULATION OF SURVEILLANCE PRACTICES

In 1978, Congress enacted the first comprehensive statute to regulate national security surveillance law, the Foreign Intelligence Surveillance Act.[9] The core mechanism of FISA is the process of regulation by ex parte court orders. To understand FISA and the case for a rule of narrow interpretation, it is necessary to understand both the theory behind regulating surveillance practices using ex parte court orders and the challenges of doing so in the specific context of national security. This Part begins by explaining the basic theory of ex parte regulation. It then turns to the conditions of successful use of that approach, and it concludes with a discussion of how national security surveillance creates an ongoing need for reform of surveillance rules.

A. Ex Parte Court Orders and the Privacy/Security Balance

When lawyers envision the judicial function, they ordinarily imagine decision makers ruling in adversarial disputes.[10] One side brings a claim. The other side denies liability. The judge rules for one side and against the other. The losing side can appeal, and the case can proceed all the way to the supreme court. The appellate courts settle the law, adopting legal interpretations that govern future disputes.[11] We can call this the adversarial model of a lawmaking court. It features two adversarial sides, and it places the judiciary in the role of decision maker between them.

Although this is the common understanding of the judicial function, there is a second role for courts that is used widely in surveillance law. The second role is that of an ex parte court that reviews court order applications. When the law regulates using ex parte court orders, no surveillance or government investigation is permitted unless the government first obtains pre-approval from a judge (often referred to in this context as a "magistrate"). The government must go to the magistrate and apply for an order allowing surveillance. If the legal requirements of the court order have been satisfied, the magistrate signs the order and the surveillance can occur. If the legal requirements of the court order have not been satisfied, the magistrate must refuse to sign the order and the

[9] See 1 Kris & Wilson, supra note 2, § 4:1, at 116.

[10] This is the traditional role described in Abram Chayes, The Role of the Judge in Public Law Litigation, 89 Harv. L. Rev. 1281, 1285–86 (1976).

[11] See id.

surveillance cannot occur. We can call this method ex parte regulation. It features only one side, and it places the reviewing judge in a largely ministerial role of determining if the legal requirements of an application have been satisfied.[12]

Modern surveillance statutes make frequent use of ex parte regulation to try to strike an optimal balance between privacy and security.[13] On one hand, surveillance protects the public by informing the government of threats and dangers. On the other hand, surveillance invades privacy and threatens civil liberties.[14] Ex parte regulation attempts to optimize the privacy/security balance by allowing surveillance when the expected benefit to security outweighs its harm to privacy. The conditions of surveillance are set by some legal decision maker, which in the case of statutory regulation is the legislature. The decision maker tries to set the conditions of surveillance so that the more severe the privacy invasion, the higher the showing required by the law. Ideally, if the threshold for obtaining a court order has been set properly, reviewing magistrates should allow surveillance when the security benefits outweigh the privacy harms but prohibit surveillance otherwise.

Consider how this works with the well-known example of a probable cause search warrant under the Fourth Amendment.[15] When the Fourth Amendment requires a warrant, a government agent must come to the judge with an application. The government must establish the constitutional requirements of probable cause and particularity.[16] Probable cause establishes the government's interest in the search by showing good reasons to think the search will be successful.[17] The particularity requirement shows that the search will be relatively narrow, as it will be limited

[12] See Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241, 1260–77 (2010) (discussing the usual procedures for ruling on warrants).

[13] For statutory examples, see 18 U.S.C. § 2703(a) (2012) (requiring a warrant to obtain e-mail); id. § 3121 (requiring a court order to obtain a pen register). The primary constitutional example is found in the text of the Fourth Amendment: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV.

[14] See Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1939–52 (2013).

[15] See U.S. Const. amend. IV.

[16] See id.; see also Fed. R. Crim. P. 41(a) (permitting a federal judge to issue a warrant based on probable cause and particularity).

[17] See Illinois v. Gates, 462 U.S. 213, 238 (1983) (defining probable cause in the case of a search warrant as "a fair probability that contraband or evidence of a crime will be found in a particular place").

to a specific place and specific evidence.[18] When probable cause and particularity have been satisfied, the resulting search should, on average, result in a benefit to the government that outweighs the privacy invasion. In the argot of Fourth Amendment law, the search will be constitutionally reasonable.

Importantly, the imposition of an ex parte court order requirement envisions a narrow role for the magistrate tasked with reviewing the application. In the case of a constitutional requirement such as a traditional Fourth Amendment warrant, the text of the Fourth Amendment defines the required showing.[19] The reviewing magistrate's job is only to say if the standard has been met.[20] In the case of a statutory regime, the legislature drafts the statute with specific thresholds for the government to satisfy that reflect the legislature's weighing of the privacy and security values implicated by the surveillance. The role of the reviewing magistrate is limited; the magistrate only determines if the threshold facts have been shown.[21] The policy-making task of setting that threshold is up to the rule maker, not the reviewing magistrate. The magistrate serves an essentially ministerial role of making sure that no orders will issue unless the rule maker's standards have been satisfied.

B. Conditions of Successful Ex Parte Regulation

Ex parte court orders can provide a stable and effective way to balance privacy and security when two related criteria are met. The first condition of successful ex parte regulation is the existence of a feedback mechanism. In any surveillance system, there must be some way of knowing how the rules are working in practice. In general, however, ex parte regulation generates no feedback.[22] Reviewing magistrates decide to grant the applications or reject them. When they reject applications, they do not write opinions explaining why. If a judge denies a warrant

[18] See Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[19] See U.S. Const. amend. IV.

[20] See Abraham S. Goldstein, The Search Warrant, the Magistrate, and Judicial Review, 62 N.Y.U. L. Rev. 1173, 1196 (1987) ("The few cases . . . hold that a judge has a 'ministerial' duty to issue a warrant after 'probable cause' has been established.").

[21] See id.

[22] There are some narrow exceptions. For example, under Federal Rule of Criminal Procedure 41, the agents must file a return on the warrant with the issuing magistrate that informs the magistrate what property was seized pursuant to the warrant. Fed. R. Crim. P. 41(f)(1)(D) ("The officer executing the warrant must promptly return it—together with a copy of the inventory—to the magistrate judge designated on the warrant.").

application, the denial is not an appealable final order.[23] There is no case to appeal. And when magistrates grant applications, they merely sign the orders. With the order issued, the magistrate's task is done.

Because the ex parte process does not itself generate feedback, the functioning of an ex parte regulatory system requires an alternative method of oversight. Consider the Fourth Amendment's exclusionary rule, which can provide for suppression of evidence when the government obtains evidence in violation of the prohibition on unreasonable searches and seizures.[24] Ex ante, judges review warrant applications and sign them to approve searches. But the primary feedback mechanism is ex post review. After a warrant is issued, leads to a successful search, and then results in criminal charges, the defendant can move to suppress the evidence and ask the reviewing court to assess ex post whether investigators violated the Fourth Amendment.[25]

Under an exclusionary rule, ex post review shifts the judicial function from that of ex parte regulation to the classic adversarial model of a lawmaking court. The defendant will claim that the law was violated, and the government will disagree. The court will author an opinion explaining the facts and reaching a decision, and the loser can later appeal that ruling up through the appellate courts. Published decisions on how the investigators acted provide courts and legislators with feedback about how the law is working in practice.

The second condition of stable ex parte regulation is technological stability. The basic thinking behind ex parte regulation is that a specific kind of surveillance will generally be worthwhile when a specific factual predicate has been satisfied. When technology remains stable, the kind of surveillance and the nature of the factual predicate will remain constant and relatively clear. The balance implicit in the statute stays steady over time. Again, consider a warrant to search a home based on probable cause. What it means to search a home has remained fairly constant over time. The act of searching a home for evidence in the eighteenth century

[23] See United States v. Savides, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), aff'd sub nom. United States v. Pace, 898 F.2d 1218 (7th Cir. 1990). But see In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 605 (5th Cir. 2013) (concluding that the government may appeal the denial of an ex parte court order for historical cell site information sought under 18 U.S.C. § 2703(d)).

[24] See generally 3 Wayne R. LaFave et al., Criminal Procedure § 9.4(b) (3d ed. 2007) (describing the exclusionary rule).

[25] See id.

is basically the same as it is in the twenty-first century.[26] And the kinds of facts that constitute probable cause today are essentially the same as in earlier generations. As a result, the ancient rule that the government needs probable cause and a warrant to search a home remains a viable and clear rule.

That balance becomes unstable, however, if technology is in flux. If the technological facts of surveillance change, the invasiveness of surveillance changes along with it. On paper, the legal rule will look the same. But in practice, changing technology can dramatically alter the significance of the rule. Two related problems emerge. First, as the technological facts change, the rule may end up allowing a vastly different amount of surveillance than was assumed when the rule was initially created. Second, the meaning of the law itself can become uncertain. Existing language that defines the government's burden in one technological era may become quite fuzzy in another technological era. New facts will create significant ambiguities as to how the old legal standard applies.

The second problem is particularly troubling for the problem of national security surveillance law, and an example may be helpful to demonstrate the point. Consider the scope of the Pen Register statute in the dawn of the Internet era. In 1986, Congress enacted the Pen Register statute as part of the Electronic Communications Privacy Act to create privacy protection that limits the real-time acquisition of communications network metadata.[27] At the time, Congress was focused on the telephone network. The U.S. Supreme Court had held in *Smith v. Maryland* that the government could install a pen register to learn the numbers dialed from a telephone without triggering the Fourth Amendment.[28] The Pen Register statute stepped into the space *Smith* left unregulated by requiring a court order before investigators could order the phone company to collect the numbers dialed from a telephone.[29]

[26] See Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 517–18 (2011).

[27] See 18 U.S.C. §§ 3121–3127 (2012). The Pen Register statute was passed as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301(a), 100 Stat. 1848, 1868–72 (codified as amended at 18 U.S.C. §§ 3121–3124, 3126–3127 (2012)).

[28] 442 U.S. 735, 745–46 (1979).

[29] From 1986 to 2001, the definition of "pen register" in the statute was telephone-specific: The law defined a pen register as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." 18 U.S.C. § 3126(3) (Supp. V 1986) (amended 2001); cf.

Starting in the 1990s, however, the question arose whether the Pen Register statute also applied to the Internet.[30] As a policy matter, it made eminent sense that it would. Otherwise there was no privacy law at all that limited government access to Internet metadata collected in real time. But the 1986 language was not drafted with the Internet in mind and contained at least some apparently telephone-specific text.[31] As a result, it was a close call, purely as a matter of statutory interpretation, as to whether the privacy law applied beyond the telephone context.[32] Congress eventually stepped in to resolve the ambiguity and extended the statute to the Internet,[33] in part due to an unpublished magistrate judge's opinion, unknown outside the government, holding that the statute did not apply to the Internet.[34] But before the law was amended, the old text left the application of the law to an important new technology surprisingly unclear. And despite the obvious importance of the question, few outside the small circle of surveillance law nerds even knew the question existed until Congress publicly amended the statute in 2001.

C. FISA and the Conditions of National Security Surveillance

Now let's turn to the Foreign Intelligence Surveillance Act.[35] As enacted in 1978, its purpose was to replace the prior regime of surveillance regulated only by the Fourth Amendment with a new system of ex parte court order regulation adapted from the law of criminal investigations.[36] In its original form, it required a wiretapping order, modeled off of the criminal law Wiretap Act, before the government could wiretap agents of foreign powers in the United States.[37] Over time, FISA expanded its use of ex parte orders. It added an ex parte order requirement for the na-

United States v. Guglielmo, 245 F. Supp. 534, 535 (N.D. Ill. 1965) ("The pen register is a mechanical device attached on occasion to a given telephone line, usually at central telephone offices. A pulsation of the dial on a line to which the pen register is attached records on a paper tape dashes equal to the number dialed.").

[30] Orin S. Kerr, Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't, 97 Nw. U. L. Rev. 607, 632–36 (2003).

[31] The competing arguments are explained in detail in id.

[32] See id. at 632–33.

[33] See id. at 636–38.

[34] See id. at 635 (citing In re United States, Cr.-00-6091 (N.D. Cal. Nov. 17, 2000) (Trumbull, Mag. J.) (unpublished opinion)).

[35] 50 U.S.C. §§ 1801–1871 (2012).

[36] See 1 Kris & Wilson, supra note 2, §§ 3.6–3.7, at 102–08.

[37] See Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1811 (2012)).

tional security equivalent of physical searches pursuant to warrants in 1994,[38] and for the national security equivalent of grand jury subpoenas and pen registers in 1998.[39] In 2007 and 2008 amendments, it added blanket court orders of individuals believed to be located outside the United States.[40] For all of these court orders, the executive branch must apply for an order before a special court of appointed federal district judges, meeting as part-time members of the FISC, to obtain approval.

In light of the prior discussion, we can see that the conditions of foreign intelligence surveillance pose significant problems for ex parte regulation. The first problem is technological. Communications network technology changes rapidly, and the national security agencies are at the leading edge of technological change. The second problem is the absence of a strong, democratically accountable feedback loop to monitor how the laws are working in practice.

For agencies like the National Security Agency ("NSA"), technological advantage is critical. The country's national security apparatus has an extraordinarily large budget, and it uses the most advanced technology to conduct surveillance and analysis of foreign intelligence.[41] The NSA follows wherever communications technology goes, seeking to acquire that information, store it, and analyze it with an efficiency and capability unknown in the private sector. And the advent of computers and the Internet have made technological change a constant. For most users, the changes are imperceptible. The telephone and the Internet just work, as if by magic. But for the computer geeks that help run national security surveillance, it is what happens behind the scenes that matters. Surveillance experts focus on how the network actually works and what powers the government has to monitor the traffic over it. The internal perception of users is irrelevant. And from the expert perspective, both the Internet

[38] See Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3423, 3443–53 (1994) (codified as amended at 50 U.S.C. §§ 1821–1829 (2012)).

[39] See Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, §§ 601–602, 112 Stat. 2396, 2404–12 (1998) (codified as amended at 50 U.S.C. §§ 1841–1846, 1861–1862 (2012)).

[40] See Protect America Act of 2007, Pub. L. No. 110-55, §§ 2–3, 121 Stat. 552, 552–55; FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2437–58 (2008) (codified at 50 U.S.C. §§ 1881a–1881g (2012)).

[41] According to the classified budget documents released by Edward Snowden, the NSA was scheduled to receive $10.5 billion in 2013. See Barton Gellman & Greg Miller, "Black Budget" Revealed: Top-Secret Summary Details U.S. Spy Network's Successes, Failures and Objectives, Wash. Post, Aug. 29, 2013, at A1.

and technological surveillance tools are constantly morphing and relentlessly dynamic.[42]

Second, national security surveillance lacks a natural alternative feedback loop to inform Congress of how its surveillance rules are working. The goal of national security surveillance is the collection of information that can be used inside the government but ordinarily will not be publicly disclosed. Unlike the criminal process, there is no obvious end of the road when the case is over, the evidence comes out, and ex post review can occur. When the government collects information for national security purposes, it is a one-way street. The government gets the information, and it is never seen again.[43]

Congress has addressed the absence of a natural feedback loop by requiring the executive to provide classified briefings about intelligence efforts to members of the House and Senate Intelligence and Judiciary Committees. Specifically, 50 U.S.C. § 1871(a) requires the Attorney General to provide semi-annual reports to these committees that provide members information, including "a summary of significant legal interpretations of this chapter involving matters before the Foreign Intelligence Surveillance Court or the Foreign Intelligence Surveillance Court of Review"[44] as well as "copies of all decisions . . . or opinions of the Foreign Intelligence Surveillance Court or Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of the provisions of this chapter."[45] The basic idea is to strike a balance between protecting vital secrets and democratic accountability by informing members of the major committees but not the Congress as a whole nor the public.[46]

[42] I recently documented some of the changes in Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 390–410 (2014).

[43] Even if court challenges are brought, they rarely succeed. In many cases, the state secrets doctrine will block civil suits designed to obtain rulings on surveillance practices. See Laura K. Donohue, The Shadow of State Secrets, 159 U. Pa. L. Rev. 77, 84–88 (2010). Under the state secrets privilege, courts can reject civil suits if the litigation would reveal valuable intelligence information. See id. at 82. In effect, the common path of civil litigation is closed in order to keep the government's secrets confidential. Once again, there is no feedback loop: The design of national security surveillance is to avoid published opinions explaining surveillance practices and how they work. See id. at 84–85.

[44] 50 U.S.C. § 1871(a)(4) (2012).

[45] Id. § 1871(a)(5).

[46] See L. Elaine Halcin & Frederick M. Kaiser, Cong. Research Serv., RL32525, Congressional Oversight of Intelligence: Current Structure and Alternatives (2012), available at http://assets.opencrs.com/rpts/RL32525_20120314.pdf.

Although well-intentioned, these limited disclosures fail to generate the necessary feedback about what the law authorizes. That is true for two reasons. First, elected representatives are poorly equipped to represent majority preference when the public is intentionally left in the dark. Elected representatives briefed on classified programs may not understand the programs themselves. Even if they understand the programs, they will not know how the public would react. It is particularly challenging to predict responses to secret surveillance programs the public cannot readily imagine based on technologies few even know exist. Plus, elected officials will not know if the public will ever learn of the programs to make predicted public reaction particularly salient. Awareness of eventual disclosure focuses attention on the likely public response. Its absence directs attention elsewhere.

Further, even if disclosure to Congress as a whole were sufficient, disclosure to specific committees raises special problems. The membership of the Judiciary and Intelligence Committees are not picked at random.[47] Over time, the committee membership may develop a close relationship with the agencies they oversee.[48] And it may be difficult for members of the relevant committees to persuade the Congress as a whole of the need for reform. None of this denigrates the hard work and careful attention that these committees provide to oversight of national security surveillance. Such oversight can be particularly effective when focused on compliance with the law. At the same time, disclosure limited to specific committees does not create feedback necessary to ensure the democratic accountability of surveillance law itself.

Ex parte regulation works best with transparent practices and stable technology. National security surveillance offers the worst of both worlds, with secret practices and rapid technological change. Obsolete and uncertain legal restrictions are inevitable. The key question is how the law will deal with the ambiguities and obsolescence.

[47] See id. at 6–7; see also Frequently Asked Questions About Committees, U.S. Senate, http://www.senate.gov/general/common/generic/committee_faq.htm#committee_assignment (last visited May 5, 2014) ("Each party assigns, by resolution, its own members to committees, and each committee distributes its members among subcommittees.").

[48] See, e.g., Lauren Fox, Spy Game: Why Congress Is Limited in Its CIA Oversight, U.S. News & World Rep. (Mar. 12, 2014, 5:33 PM), http://www.usnews.com/news/articles/2014/03/12/spy-game-why-congress-is-limited-in-its-cia-oversight ("In the years since the Sept. 11 terrorist attacks, the intelligence community has maintained a cozy relationship with the Senate Intelligence Committee tasked with overseeing its activities.").

II. THE FISC AND THE FAILURE OF THE HYBRID APPROACH

The leaks beginning in the summer of 2013 revealed the operation of the FISC for the first time. Edward Snowden leaked several documents, and the public reaction pushed the Obama administration to release redacted versions of FISC opinions. The unearthed decisions revealed that the FISC had assumed a new role. Although designed as an ex parte court tasked primarily with reviewing court order applications, the FISC had secretly taken on an additional important role of a lawmaking court. The resulting hybrid placed the FISC in a position akin to an executive agency with broad powers to regulate national security law.

Equally importantly, the released FISC opinions revealed that the FISC had interpreted the surveillance laws in surprising and perhaps shocking ways. Technological change had destabilized key aspects of FISA and created ambiguities that the FISC then tried to resolve.[49] Because no public feedback loop existed, the FISC's interpretations had remained secret. And acting in secret, the FISC had issued opinions approving programs far removed from the statutory text that astonished the public when the Snowden disclosures made them public.

This Part explains the new hybrid role of the FISC revealed by Snowden's disclosures. Acting in secret, the FISC transformed itself into a novel mixture of an ex parte court and an adversarial court that effectively created the legal standards for national security surveillance law. The result has been a body of secret law that seems removed from what a majority of the public would approve.[50] That novel role for the FISC has triggered a set of proposed legislative responses. This Part concludes by introducing the major legislative proposals to reform the FISC, all of which try to make the FISC a better-functioning hybrid court.

---

[49] See infra Section II.B.

[50] Confident conclusions about public opinion are difficult because relatively few members of the public understand the details of individual surveillance programs and polling questions are often imprecise. Nonetheless, public opinion on NSA surveillance practices generally has tended to poll slightly negative in the wake of Snowden's disclosures. When asked in a January 2014 Pew Research Center/USA Today survey, "Overall, do you approve or disapprove of the government's collection of telephone and internet data as part of anti-terrorism efforts?", 53% disapproved and 40% approved. See Pew Research Ctr., Obama's NSA Speech Has Little Impact on Skeptical Public: Most Say U.S. Should Pursue Criminal Case Against Snowden 12 (Jan. 20, 2014), available at http://www.people-press.org/files/legacy-pdf/1-20-14%20NSA%20Release.pdf; see also Letter from Senators Ron Wyden & Mark Udall to Attorney Gen. Eric Holder 1 (Mar. 15, 2012), available at http://www.fas.org/irp/congress/2012_cr/wyden031512.pdf ("We believe most Americans would be stunned to learn the details of how these secret court opinions have interpreted section 215 of the Patriot Act.").

A. The Hybrid Role of the FISC Exposed

Until the summer of 2013, almost all of the FISC's work product remained highly classified. Every year, the Justice Department ("DOJ") released a one-to-two-page summary reporting the number of FISC orders that the government had applied for and the court had granted.[51] But these summaries shed almost no light on the work of the FISC. Even the fact that almost every FISC application recorded was granted was a source of mystery, as the published figures do not indicate whether the FISC judges work with the DOJ lawyers informally to consider possible applications before formal applications are made.[52]

Most importantly, it was not public what (if anything) the FISC did beyond approve or disapprove the government's applications to conduct surveillance. Did the FISC issue opinions? Did it conduct substantive review of surveillance practices? No one in the general public knew the answers. The traditional role of ex parte and ex ante review is merely to review applications and either sign or refuse to sign orders. Ex parte review normally does not generate case law or lead to opinions. But until the summer of 2013, the work of the FISC remained secret—both as to whether the FISC had exceeded the traditional role of an ex parte court and if so, how the FISC had regulated the executive branch and what legal interpretations it had adopted.

The flurry of Snowden documents changed that. Starting in the summer of 2013, several documents from the FISC were disclosed.[53] And in response to Snowden's leaks, the federal government released additional troves of FISC materials.[54] The documents revealed that the FISC had indeed issued legal opinions on its surveillance powers. When faced with an application for surveillance based on a questionable reading of its powers, the FISC had issued opinions interpreting its authorities.

[51] The reports are available at FISA Annual Reports to Congress, Fed'n of Am. Scientists, http://www.fas.org/irp/agency/doj/fisa/#rept (last visited May 12, 2014).

[52] In 2012, 1789 applications to conduct electronic surveillance were made before the FISC. One application was withdrawn, and 1788 were approved, 40 with modifications. See Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., to Harry Reid, Senate Majority Leader, 2012 FISA Annual Report to Congress (Apr. 30, 2013), available at http://www.fas.org/irp/agency/doj/fisa/2012rept.pdf.

[53] See Harding, supra note 1. The disclosures began on June 5, 2013. Volz, supra note 1.

[54] David S. Kris, On the Bulk Collection of Tangible Things 6–8 (Lawfare Research Paper Series, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf.

FISC opinions also engaged in extensive oversight of the NSA's compliance with its earlier orders[55]

The FISC's opinions that regulated the FISC were striking in their content and form. First, the quality of the FISC's legal analysis was surprisingly poor. The FISC had authorized vastly more surveillance than outside observers could have imagined based on the public text of the statute. In the hands of the FISC judges, acting in secret, the text of FISA was no longer a reliable guide to executive branch authority.

B. The FISC's Work Product Revealed

The most important example of the FISC's weak decision making is the FISC's approval of the bulk telephony metadata program under Section 215 of the USA Patriot Act.[56] Section 215 is a national security analog to the traditional grand jury subpoena power in criminal investigations. In criminal cases, grand juries (generally controlled by prosecutors) can order third parties to hand over documents as long as compliance is not overly burdensome and the materials sought are relevant to a criminal investigation.[57] Grand jury subpoenas are not self-executing, however. Although issued by prosecutors in the name of the grand jury, the recipient of a subpoena can challenge a subpoena before a judge prior to compliance.[58]

On its face, Section 215 contemplates a similar power for national security investigators. It allows the government to obtain a court order from third parties for any tangible things under the traditional standards for subpoenas.[59] Section 215 employs one significant modification of the usual process for grand jury subpoenas: The judicial review occurs automatically at the outset so that the court must sign off on the request at the beginning instead of waiting for a later challenge.[60] Despite this difference, the Section 215 authority is expressly limited to that which any federal prosecutor would have in a criminal case. According to the stat-

[55] See, e.g., In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *7, *9–10 (FISA Ct. Aug. 29, 2013) [hereinafter In re FBI Application].

[56] USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861 (2012)); see also In re FBI Application, supra note 55, at *7–10 (approving the bulk telephony metadata program).

[57] See 3 LaFave et al., supra note 24, § 8.7, at 151–77.

[58] See In re Horowitz, 482 F.2d 72, 75–80 (2d Cir. 1973).

[59] 50 U.S.C. § 1861(c) (2012); see 3 LaFave et al., supra note 24, § 8.7, at 151–77.

[60] 50 U.S.C. § 1861(c)(1).

ute, a court may issue a Section 215 order only if the tangible thing obtained could "be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation."[61] In other words, if a federal prosecutor in Topeka or San Antonio could not issue a lawful grand jury subpoena for the records, the FISC could not enter an order requiring a third party to hand over those records under Section 215.

Despite this limitation, the FISC ruled that Section 215 authorized an astonishing program: It enabled the government to obtain individual orders requiring telephone providers to hand over certain non-content records of *all* telephone calls of *all* of its customers, in real time.[62] Telephone companies with tens of millions of customers had been secretly handing over *telephone records of all of its customers for years*, all pursuant to bulk Section 215 court orders that covered tens of millions of customers—and with all of the calls they made, presumably billions of telephone call records—at once.[63] The government then queried the database when it had reasonable suspicion to believe that a particular number was involved in terrorist activity, obtaining the records of that number, the records of any number in contact with that number, and the records of any number in contact with the numbers in contact with the original number.[64]

As a practical matter, the FISC had created its own surveillance authority. On its face, Section 215 simply authorized a national security subpoena power.[65] But by blending the roles of ex parte court and adversarial court, the FISC had interpreted FISA to authorize a new kind of program: a collect-it-all-and-query-with-suspicion model that bore no particular resemblance to the statute that purported to justify it. The FISC's interpretation obviated the need for the executive branch to seek express legislative approval for new programs. And it did this entirely in secret, leading to a massive surveillance program the very nature of which was unknown and unknowable to the public.

[61] Id. § 1861(c)(2)(D).

[62] See Administration White Paper, Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act 2–5 (2013), archived at http://perma.cc/8RJN-EDB7; Kris, supra note 54, at 2–3.

[63] See Kris, supra note 54, at 2–6.

[64] See id. at 10–12.

[65] 50 U.S.C. § 1861(c).

How had this come to pass? The key difficulty was that technology had outpaced the law. The limits of the subpoena power are well established except in one important respect: their application to computerized records. Subpoenas must seek relevant information, but sometimes that relevant information can be hidden in a database. Lower courts have entered divided opinions on whether and when a subpoena can be used to obtain a database to be searched later on for the relevant information. On one hand, courts have held that, in principle, the subpoena power can be used in that way.[66] At the same time, courts have indicated that there are limits on how far this power can go.[67] For example, the power can only be used when necessary, based on whether it is possible to obtain the relevant records some other way.[68]

The FISC opinions harnessed this ambiguity to approve a program far removed from the statutory text. As summarized in an opinion by Judge Eagan,[69] the FISC reasoned that the government could subpoena every phone record all at once because it appeared necessary to do so. Why did it appear necessary? Here, the FISC simply recited the statements offered by the executive branch.[70] The Justice Department informed the FISC that in its view, it was necessary to have all telephony metadata in order to do effective analysis of that metadata and identify terrorist suspects.[71] The FISC accepted this assertion as true,[72] effectively assuming the key fact based on the government's say-so.

At bottom, the FISC's argument was largely circular. It was legal to subpoena every phone record because it was necessary to do so to achieve the legitimate aim of the statute; and it was necessary to do so

[66] See, e.g., Carrillo Huettel, LLP v. SEC, No. 11cv65-WQH (CAB), 2011 WL 601369, at *2 (S.D. Cal. Feb. 11, 2011).

[67] In re Grand Jury Subpoena Duces Tecum Dated Nov. 15, 1993, 846 F. Supp. 11, 13–14 (S.D.N.Y. 1994).

[68] Id. at 13.

[69] In re FBI Application, supra note 55, at *7, *9.

[70] See id. at *7.

[71] See id.

[72] After reciting the government's claim, Judge Eagan writes:

> The fact that international terrorist operatives are using telephone communications, and that it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations, is sufficient to meet the low statutory hurdle set out in Section 215 to obtain a production of records.

Id. Judge Eagan provides no further analysis, effectively accepting the government's assertion of necessity on its face.

because the government claimed that the program was the only way to identify terrorists effectively. In other words, the program was legal because the government claimed it was effective. As construed in secret by the FISC, the government could obtain any database as long as the government secretly claimed that it needed the database. Because Section 215 incorporates the subpoena standard,[73] and the FISC had interpreted the subpoena standard to allow bulk collection, the FISC interpreted Section 215 to authorize the bulk collection program.

Whatever the merits of the bulk telephony metadata program as policy, the text of Section 215 does not authorize it. For the FISC to be correct, any federal prosecutor anywhere in the country could have compelled every phone company to hand over all of its telephony metadata on an ongoing basis so long as the prosecutor claimed that it was necessary to help solve a case. It is hard to imagine a federal judge allowing such a subpoena in a criminal case, which would cover the records of hundreds of millions of people on an ongoing basis. And because the Section 215 authority is expressly limited based on what a federal prosecutor could subpoena, it is difficult to read Section 215 as allowing that authority in the national security surveillance context.

The FISC's allowance of bulk collection under Section 215 is just one of several examples of the weak reasoning found in the FISC opinions.[74] Taken together, the poor quality of the FISC's work product demonstrates the failure of the FISC's hybrid approach to surveillance regulation. By combining ex parte procedures with the rulemaking power of an adversarial court, the FISC created a secret body of law that bore only a weak resemblance to the public statutes that Congress enacted. The role of Congress became an afterthought.

President Obama's recent announcement that the surveillance laws should require an ex ante court order to query the Section 215 database demonstrates the scope of the problem.[75] To shift to that new legal regime, President Obama ordered the Justice Department to ask the FISC

[73] 50 U.S.C. § 1861(c)(2)(D) (2012).

[74] For another example, see Orin Kerr, Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata, Lawfare Blog (Nov. 19, 2013, 2:35 AM), http://www.lawfareblog.com/2013/11/problems-with-the-fiscs-newly-declassified-opinion-on-bulk-collection-of-internet-metadata/.

[75] See President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

to approve the new procedure, which the FISC then did.[76] No one consulted Congress. The hybrid role of the FISC rendered Congress an afterthought, sharply diminishing the role of public input through the elected branches within foreign surveillance law.

C. Proposals to Improve the Hybrid FISC

The surprising conclusions reached by the FISC have triggered many proposals to reform FISC procedures. The procedural reforms share a common theme: They aim to make the FISC more like a regular adversarial court. That is, the proposals assume that the FISC's problem is that it is an ex parte court, and that the best solution is to introduce the procedures common to an adversarial lawmaking court. With the FISC's procedures reformed, the thinking goes, the FISC will adopt more persuasive interpretations of FISA. National security surveillance law will then develop in a more predictable and accountable way.

Consider the three major types of proposals. First, many have argued that the FISC needs to add a public advocate who can argue the pro-civil liberties side before the FISC.[77] The basic idea is to help the FISC's work by making the FISC proceedings adversarial: The FISC will do better when it hears both sides. Second, many proposals would bolster the appellate structure of the FISC.[78] Under the current statute, the government can appeal when it loses.[79] But no one can appeal when the government wins. Under the reform proposals, the special advocate would have the authority to file an appeal.[80] Review could then proceed to the Foreign Intelligence Court of Review, and then, if necessary, to the U.S. Supreme Court. Third, many have argued that the FISC should

[76] See Order Granting the Government's Motion to Amend the Court's Primary Order Dated January 3, 2014 at 3–4, 9, In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109 (FISA Ct. Feb. 5, 2014), available at http://s3.documentcloud.org/documents/1017778/misc-14-01-order.pdf.

[77] Several of these proposals are summarized in a recent Congressional Research Service report. See Andrew Nolan et al., Cong. Research Serv., 7-5700, Introducing a Public Advocate into the Foreign Intelligence Surveillance Act's Courts: Select Legal Issues (2013), available at http://justsecurity.org/wp-content/uploads/2013/10/CRS-Report-FISC-Public-Advocate-Oct.-25-2013.pdf.

[78] See Raffaela Wakeman, An Overview of FISA Reform Options on Capitol Hill, Lawfare Blog (Nov. 3, 2013, 10:08 AM), http://www.lawfareblog.com/2013/11/an-overview-of-fisa-reform-options-on-capitol-hill/.

[79] The first appeal to the Foreign Intelligence Court of Review was *In re Sealed Case*, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

[80] Wakeman, supra note 78.

publish its opinions—or at least summaries of its opinions—so the public is put on notice about the legal interpretations the FISC has adopted.[81]

These three proposals share the assumption that the FISC should continue to serve as a lawmaking court. On one hand, the proposals maintain the FISC as an ex parte court in structure: The government continues to go to the FISC to seek approvals of court orders. On the other hand, they try to introduce adversarial mechanisms that are thought to generate reliable decision making. Underlying these mechanisms is the assumption that the FISC should be making law in its decisions.

Of course, not every application will raise difficult interpretive issues. But when the government does come to the FISC with an application based on an aggressive reading of the law, the assumption goes, the FISC should enter a ruling. The proposals for reform simply try to improve the environment in which this occurs. At the very least, the thinking goes, there should be some sort of briefing on the other side in some cases. At the very least, there should be some kind of appeal, at least in some cases. And at the very least, there should be some sort of public notice of the interpretation that the FISC has adopted. The reforms accept the FISC as a hybrid between an ex parte court and a lawmaking court, and they try to create better conditions for lawmaking.

III. A RULE OF LENITY FOR NATIONAL SECURITY SURVEILLANCE LAW

This Part introduces a different way to improve national security surveillance law. The better solution is to adopt a rule of lenity for judicial interpretations of the national security surveillance statutes. When courts interpret those laws, ambiguity should be construed in favor of the citizen and against the State. This rule would allow Congress to revisit the national security laws and decide whether to give the executive branch specific powers that it may seek. But that task properly belongs to Congress rather than the courts. Updating the surveillance laws should occur in public view with public feedback. Narrow judicial construction will encourage that dynamic by revising the role of the different branches in national security surveillance law. The Snowden disclosures revealed that the FISC has placed itself in charge. A rule of lenity would limit the role of the FISC and place the primary responsibility for rulemaking

[81] See id.

where it belongs: with the people, acting through their elected representatives.

This Part makes the case for a rule of lenity in four steps. First, it introduces the rule of lenity from criminal law as an example of an interpretive rule that construes executive power narrowly. Second, it argues that Congress should borrow the basic approach of a rule of lenity from criminal law and apply it to national security surveillance law by enacting a new statute that provides interpretive guidance to the courts. Third, it explains the three major benefits of such an approach: It would encourage transparency and accountability; it places decision-making authority in the branch best suited to balance privacy and security; and it avoids the constitutional and practical difficulties with existing reform proposals. The Part concludes by considering how the proposal would work in practice. In particular, it responds to the objection that such a proposal would make no difference because courts could simply ignore it.

A. The Rule of Lenity in Criminal Law

The rule of lenity is a principle of interpretation used for construing ambiguous criminal statutes. Under the rule, "[A]mbiguity concerning the ambit of criminal statutes should be resolved in favor of lenity."[82] When the legislature has not spoken clearly as to what is punished, the rule of lenity breaks the tie in favor of the individual instead of the State.[83] Of course, where the meaning of a statute can be determined from the usual legal materials, that meaning must be adopted. But when language in criminal statutes is subject to several fair interpretations, the rule of lenity directs that courts adopt the narrow interpretation.

The rule of lenity is rooted in the separation of powers. It reflects the fundamental directive that legislatures, not courts, should have the primary role in determining what is a crime. Crimes reflect the judgment of the public as expressed through its legislature: Criminal offenses are charged in the name of *The People*. The rule of lenity helps ensure democratic accountability by directing courts not to engage in common-law decision making about the scope of criminal conduct.[84] Of course, legis-

[82] Rewis v. United States, 401 U.S. 808, 812 (1971).

[83] See, e.g., United States v. Canal Barge Co., 631 F.3d 347, 353 (6th Cir. 2011).

[84] See Zachary Price, The Rule of Lenity as a Rule of Structure, 72 Fordham L. Rev. 885, 886 (2004).

latures can revisit statutes and broaden them through the legislative process.[85] But the rule of lenity aims to ensure that the broadening reflects the public input of the legislature, not the decisions of unaccountable judges. In so doing, it limits the scope of government power to what an ordinary citizen might understand upon following the work of the legislature and reading the rules it enacts.[86]

Consider a classic example of the rule of lenity, *McBoyle v. United States*.[87] The defendant had transported an airplane across state lines that he knew had been stolen.[88] The government charged the defendant with interstate transportation of a "motor vehicle," a term defined by statute as "an automobile, automobile truck, automobile wagon, motor cycle, or any other self-propelled vehicle not designed for running on rails."[89] The question before the Court was whether an airplane counted as a "self-propelled vehicle not designed for running on rails," and specifically whether an airplane was a "vehicle."[90]

Writing for a unanimous Court, Justice Holmes concluded that an airplane was not a vehicle for purposes of the statute and therefore ruled in favor of the defendant.[91] As a matter of policy, Justice Holmes noted, it would be sensible to include airplanes within the statute's prohibition. Indeed, "if the legislature had thought of it," Holmes speculated, "very likely broader words would have been used."[92] But the judicial role was narrower:

> Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.[93]

[85] Subject to the void for vagueness doctrine, of course. See, e.g., City of Chicago v. Morales, 527 U.S. 41, 56–64 (1999).
[86] See Price, supra note 84, at 886–88.
[87] 283 U.S. 25 (1931).
[88] Id.
[89] Id. at 26.
[90] Id. at 25–26.
[91] Id. at 27.
[92] Id.
[93] Id.

Justice Holmes therefore read the term "vehicle" in its more natural and common way to mean mode of transportation on land.[94] The policy question of whether airplanes should be included was left to a future Congress.

B. Adopting A Lenity Rule for Surveillance Law

The principle of the rule of lenity should be adapted to apply in the context of national security surveillance law. Congress should adopt a rule of narrow judicial interpretation when courts are called on to interpret the scope of government power those laws grant. Ambiguity in the scope of the national security surveillance statutes should be construed against the government. The tiebreaker should go to the individual, not the State. Under this approach, courts would be unable to engage in common-law decision making designed to make policy or resolve difficult legislative questions. The hybrid FISC role would be rejected. Instead, the FISC would stay out of lawmaking and defer to Congress. If the executive concluded that the laws were out of date, it would be up to the executive to go to Congress, rather than the FISC, to seek an amendment.

A rule of lenity for national security surveillance law would distribute power properly among the branches of government, much as it does in the context of criminal law. It would reflect the fundamental directive that legislatures, not courts, should have the primary role in determining what executive branch action complies with the law. National security surveillance statutes reflect the judgment of the public as expressed through its legislature. An appropriate interpretive rule can help ensure this distribution of power by directing courts not to engage in common-law decision making about the scope of surveillance powers conduct. Of course, Congress would be free to revisit statutes and broaden them through the legislative process. The President's role in proposing and approving legislation, and the recognition of his Article II authority as Commander in Chief,[95] would ensure significant influence on congressional output. But the rule of lenity would ensure that the broadening re-

[94] See id.

[95] U.S. Const. art. II, § 2, cl. 1 ("The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the United States . . . .").

flects the public input of the legislature, not the decisions of unaccountable judges.

The interpretive rule would be created by express statutory enactment. It could be fairly simple to draft and enact. Congress could simply pass a new section of Chapter 36 of Title 50, the chapter reserved for national security surveillance, along these lines:

> *50 U.S.C. § 1886: Rule of Lenity*
>
> *The scope of government powers permitted by this chapter shall be construed narrowly.*

Congress has the constitutional authority to enact such an interpretive rule. Scholars have debated whether Congress could enact principles of judicial interpretation that would apply to the entire U.S. Code all at once.[96] Professor Tribe argues that Congress has no such authority, at least as applied prospectively, as it would allow one Congress to improperly bind future Congresses.[97] Professor Rosenkranz disagrees and argues that Congress has such power.[98] But the rule of lenity offered here avoids this debate with its specific focus. The proposed rule of lenity would govern only a single chapter of a single title of the U.S. Code, Chapter 36 of Title 50, governing national security surveillance. Such a statute-specific provision is generally thought to be within Congress's power.[99]

Congress's interpretive rule for the Racketeer Influenced and Corrupt Organizations Act ("RICO")[100] provides a helpful example. When Congress enacted RICO, it included a rule to govern its judicial interpretation: "The provisions of this title shall be liberally construed to effectu-

[96] See Nicholas Quinn Rosenkranz, Federal Rules of Statutory Interpretation, 115 Harv. L. Rev. 2085, 2086–88 (2002) (discussing legislative power to modify canons of interpretation). An example of such a questionable interpretive rule is 15 U.S.C. § 2403(c) (2012), which states that, "The laws, rules, regulations, and policies of the United States shall be . . . interpreted as to give full force and effect" to federal policy encouraging high productivity growth in the economy.

[97] See 1 Laurence H. Tribe, American Constitutional Law § 2–3, at 126 n.1 (3d ed. 2000).

[98] See Rosenkranz, supra note 96, at 2115–20.

[99] See id. at 2119 n.146; see also Kent Greenawalt, Statutory and Common Law Interpretation 128 (2013) (concluding that such guidance should be constitutional).

[100] 18 U.S.C. §§ 1961–1968 (2012).

ate its remedial purpose."[101] The Supreme Court has referred to this rule as RICO's "liberal-construction requirement,"[102] and it has relied on Congress's directive to dictate that RICO "is to be read broadly."[103] The Supreme Court's RICO case law has not questioned Congress's power to adopt this interpretive rule, and its cases have taken the rule seriously as a guide to judicial construction.[104]

The Criminal Appeals Act, 18 U.S.C. § 3731, contains a similar interpretive rule. The statute governs when the Justice Department can appeal an adverse ruling from a federal district court, and it includes a directive that "[t]he provisions of this section shall be liberally construed to effectuate its purposes."[105] As with RICO's liberal-construction requirement, the Supreme Court and lower courts have relied on this language in adopting a broad interpretation of the executive branch's power to appeal adverse rulings.[106]

Although not enacted to govern the scope of federal executive power, the statutory clear-statement rule for preemption of state laws that regulate insurance provides another example of a congressionally mandated interpretive rule that the courts have taken seriously.[107] 15 U.S.C. § 1011 states that:

> Congress hereby declares that the continued regulation and taxation by the several States of the business of insurance is in the public interest, and that silence on the part of the Congress shall not be construed to impose any barrier to the regulation or taxation of such business by the several States.[108]

As interpreted by the Supreme Court, the provision directs courts not to hold state laws regulating the business of insurance to be preempted "unless a federal statute specifically requires otherwise."[109]

---

[101] Organized Crime Control Act of 1970, Pub. L. No. 91-452, § 904(a), 84 Stat. 922, 947 (codified as note to 18 U.S.C. § 1961 (2012)).

[102] Sedima, S.P.R.L. v. Imrex Co., 473 U.S. 479, 491 n.10 (1985).

[103] Id. at 497–98.

[104] See id.; see also Reves v. Ernst & Young, 507 U.S. 170, 183 (1993) (discussing the rule); Russello v. United States, 464 U.S. 16, 26–27 (1983) (same).

[105] 18 U.S.C. § 3731 (2012).

[106] See, e.g., Serfass v. United States, 420 U.S. 377, 387 (1975); United States v. Wolk, 466 F.2d 1143, 1146 n.2 (8th Cir. 1972).

[107] See 15 U.S.C. § 1011 (2012).

[108] Id.

[109] U.S. Dep't of Treasury v. Fabe, 508 U.S. 491, 507 (1993).

The liberal-construction requirements of RICO and the Criminal Appeals Act, as well as the clear-statement rule for the state preemption of insurance, provide significant precedents in favor of the lawfulness of an interpretive rule for FISA. That is especially so for the examples of RICO and the Criminal Appeals Act. If Congress can adopt interpretive rules broadening executive power, Congress should have the same power to adopt an interpretive rule that narrows executive power.

C. Three Benefits of a Rule of Lenity

The proposed rule of lenity offers three significant benefits. The first is democracy reinforcement. National security surveillance practices constantly change as technology advances. Technological change creates ambiguities as to the scope of government power. Some branch of government must respond to those ambiguities: either the courts or Congress, or a combination of both. A rule of narrow interpretation would force the elected legislature to play the primary role of responding to technological change. It would force decisions to be made in public by legislators who are accountable to voters instead of in secret by judges with life tenure. A rule of lenity would therefore ensure more accountable and more democratic decision making in the field of national security surveillance.

The democracy-reinforcing benefit of lenity operates in large part through transparency. Under such a rule, ambiguity created by technological change would require the executive to obtain statutory approval from Congress for new powers. The request and consideration must occur in public, as the statutory surveillance laws are public laws published in the U.S. Code.[110] Congress can then debate the executive branch's proposal, and members of the public can weigh in about how much power the executive should have. In this way, the rule of lenity fuels transparency. It enables the public to know the basic grants of authority to the executive branch, permitting a feedback loop that allows public opinion to help drive reform.

[110] The laws passed by Congress are published as the "Public Laws" of the United States. See Federal Register: About Public Law Listings, Nat'l Archives, http://www.archives.gov/federal-register/laws/about.html (last visited May 12, 2014) ("When a bill is signed into law by the President it is sent to the Office of the Federal Register to be assigned a law number and paginated for the *United States Statutes at Large*. Afterwards, a List of Public Laws is created, posted online, and then published in the *Federal Register*.").

A second benefit of the proposed interpretive approach is that it would empower the branch of government best suited to balance privacy and security as technology changes.[111] Judges are poorly suited to strike the proper balance because they struggle to understand technology.[112] Because judges also can only see issues that litigants ask them to review, they lack an institutional capacity to understand the broad contours of technological change.[113] In contrast, legislatures can hold hearings about technological change and can consult and hear from experts; they can regulate comprehensively and can readily revisit prior judgments when old technological assumptions have become outdated.[114] For these reasons, surveillance law involving new and evolving technology generally works best when Congress takes the leading role. A rule of lenity would push Congress to assume that role by directing ambiguities to be resolved legislatively instead of by judges.

The institutional advantage of Congress in the surveillance field is particularly pressing in the context of national security law. The FISC is an ex parte court staffed by trial judges.[115] The trial judges of the FISC hear only from one side, the government, and they must decide cases in secret without the advantage of amicus briefs or public commentary. Only the government can appeal. If the government makes a representation as to what rules are needed, the judges have no way to determine if the government's claims are true or false. This is an extraordinarily poor environment for policymaking. The FISC judges lack an effective way to determine what rules are optimal or how FISC-imposed rules work or fail to work. A rule of lenity recognizes this institutional disadvantage and ensures that the FISC does not play a significant role in making the policy choices required to determine how to balance privacy and security in new technology.

---

[111] See Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 805, 857–87 (2004) (discussing the "institutional limitations of judicial rulemaking" and the "significant institutional advantage" of legislatures with respect to the regulation of "criminal investigations involving new technologies").

[112] Id. at 875–82.

[113] Id. at 875–76.

[114] Id. at 875, 881–82.

[115] 50 U.S.C. § 1803(a)(1) (2012) ("The Chief Justice of the United States shall publicly designate 11 district court judges from at least seven of the United States judicial circuits of whom no fewer than 3 shall reside within 20 miles of the District of Columbia who shall constitute a court which shall have jurisdiction to hear applications for and grant orders approving electronic surveillance . . . .").

A third benefit of the rule of lenity is that it overcomes the difficult theoretical and practical problems created by FISC reform proposals that try to make the FISC more like a regular court. For example, if some kind of public advocate is appointed to argue the privacy side of cases, how should the advocate be appointed, and when should the advocate intervene? If the FISC judges have the power to appoint special advocates, they may be reluctant to appoint advocates when they want to make a quick decision in the government's favor. On the other hand, if special advocates can intervene in any case, they can bog down the process of ex parte court orders unnecessarily. Further, the Appointments Clause may place constitutional limitations on how the public advocate can be named,[116] creating a potential conflict of interest between the executive branch and the advocate tasked with challenging the executive branch.

Even more difficult issues are presented by proposals to allow for appeals filed by special advocates when the FISC adopts the government's view. First, how can a special advocate have standing to pursue an appeal?[117] What interest does the advocate represent that is sufficient to create Article III standing? If appeals are brought to the U.S. Supreme Court, is the Court supposed to receive classified briefs and hold a top secret oral argument? Given the highly classified nature of FISC proceedings and the public nature of Supreme Court review, how can FISC decisions be appealed to the Supreme Court?

Similar issues are raised by proposals to publish FISC opinions, or at least public summaries of those opinions. It may be possible to publish highly redacted opinions or summaries that merely present legal conclusions. But who decides when to release those opinions and how much they can say? If the FISC itself makes those decisions, it may err in favor of secrecy; after all, decisions that remain secret cannot be criticized. But who else can make those decisions? These problems may be solvable, but they are difficult.

A rule requiring narrow interpretation of FISA authorities would help avoid these problems. Instead of trying to improve the FISC by creating a better hybrid between an ex parte court and a regular court, a rule of lenity would limit the lawmaking power of the FISC and eliminate the need for a hybrid at all. Without substantial lawmaking powers, the

[116] See Nolan et al., supra note 77, at 8–14.
[117] See id. at 14–22.

FISC would not make the kinds of momentous decisions that require adversarial briefing, appellate review, and publication. By rejecting the rulemaking power of the FISC, a rule of lenity would eliminate the need for the adversarial apparatus necessary for reliable decision making based on an assumption of a hybrid court.

D. Predicting the Effect of a Rule of Lenity

An important counterargument to my proposal is that it might not actually work. In the criminal context, the rule of lenity often receives only lip service.[118] It is often honored only in the breach. More broadly, interpretive rules are effective only to the extent courts actually pay attention to them: Courts may simply ignore such interpretive rules or read them so narrowly as to make them irrelevant. Given these difficulties, why would we think that a rule of lenity would make a difference in the context of national security surveillance?

These are fair concerns. At the same time, I think there are three reasons to think that the statutory enactment of a rule of lenity would have a substantial effect. First, courts have relied on analogous statutory interpretive rules in the context of RICO, the Criminal Appeals Act, and federal/state preemption.[119] Indications that courts take Congress's interpretive directives seriously in those contexts suggest that they would also take such a directive seriously here. To be sure, the rule of lenity in criminal law is often ignored. But criminal law's rule of lenity is a product of judicial interpretation and background principles, not express statutory text. A statutory rule of narrow interpretation would likely have more force.

Second, congressional enactment of an interpretive rule would be a rebuke to the FISC. Adoption of such a rule would put FISC judges on notice that Congress had rejected its self-assumed role as a decision-making court. Some FISC judges might resist the rule of lenity to defend the court's prior decisions. But new appointments to the FISC would

[118] Price, supra note 84, at 886 ("Nowadays [the rule of lenity] appears occasionally as a supplemental justification for interpretations favored on other grounds; it never stands alone to compel narrow readings."); Note, The New Rule of Lenity, 119 Harv. L. Rev. 2420, 2420 (2006) ("[C]ritics explain the routine invocations of the rule of lenity as mere lip service: courts may nominally acknowledge the rule, but they find statutes to be unambiguous and therefore decline to apply it unless they would have found for the defendant on other grounds anyway.").

[119] See supra notes 100–09 and accompanying text.

know that they were joining a court that Congress had directed to stay out of the policymaking sphere. The rule of lenity would stand as a congressional directive to the FISC. It would not be impossible to ignore. But it would not be easy to ignore, either.

Third, the potential significance of a rule of narrow interpretation is suggested by the FISC's apparent adoption of a contrary rule of interpretation in the first FISC opinion to allow bulk collection of metadata. In November 2013, the Office of the Director of National Intelligence published a declassified and heavily redacted FISC opinion from 2004, authored by Judge Kollar-Kotelly, that had allowed bulk collection under a part of FISA known as the pen register provisions.[120] As I have detailed elsewhere, Judge Kollar-Kotelly's opinion offered a highly implausible reading of the relevant statutory text.[121] But overlooked in the commentary on the opinion was the rule of interpretation she invented to construe FISA broadly.

In interpreting FISA, Judge Kollar-Kotelly announced that "any ambiguity" in the statutory text should be resolved in favor of the government. This was necessary, she reasoned, because a broad interpretation would "promote the purpose of Congress"[122] in enacting the USA Patriot Act. Several provisions of the Patriot Act had been designed to loosen standards of government monitoring of non-content information. Reading the pen register provisions of FISA broadly to allow bulk collection was consistent with this general purpose, leading the court to resolve ambiguity in the government's favor.

Judge Kollar-Kotelly's interpretive method tried to help Congress achieve goals that Congress had never actually considered. It used specific statutory amendments that broadened a statute in some ways to read the statute as having been broadened in other ways. But the significance of Kollar-Kotelly's rule is that she used it to support a broad read-

[120] The case name and docket number are redacted. See FISC Opinion and Order, No. PR/TT [redacted] (FISA Ct. [date redacted]) (Kollar-Kotelly, J.), available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf; see also Press Release, Office of the Dir. of Nat'l Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Nov. 18, 2013), available at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/964-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-nov (providing links to declassified intelligence community documents including FISC opinions).

[121] See Kerr, supra note 74.

[122] See FISC Opinion and Order, supra note 120, at 18.

ing of the statute in light of the ambiguities triggered by technological change. The appearance of such a presumption to resolve ambiguity helps emphasize the extent to which the FISC's interpretive work is based on such resolutions. Just as a broad theory could assist the FISC in adopting a broad interpretation, a message from Congress directing the FISC to resolve ambiguities in favor of the individual instead of the State could assist the FISC in adopting narrow interpretations in the future.

CONCLUSION

Edward Snowden's disclosures revealed the flaws in the FISC's experiment with ex parte regulation. The FISC has taken on a hybrid role, both reviewing applications and handing down long opinions interpreting the scope of executive power as technology creates ambiguity. The existing proposals to reform the FISC embrace that hybrid role. They try to work within the role that the FISC has given itself, and to improve the context of legal decision making on the assumption that the courts must interpret what the law means.

This Essay has argued for a different approach. The best path is to reject the hybrid role of the FISC, not to try to improve it. Instead of encouraging the FISC to assume lawmaking powers, Congress should discourage that role by requiring the FISC to follow a rule of lenity. A rule of lenity would push lawmaking authority back to Congress where it belongs, encouraging public rulemaking by the body best situated to balance privacy and security. The FISC should be restored to its original role, that of an ex parte court. Such a change would not single-handedly solve the problems with national security surveillance law. But it would be a simple start that should be among the options Congress considers when it next amends the Foreign Intelligence Surveillance Act.

***