GUANTÁNAMO AND BEYOND

EXCEPTIONAL COURTS AND MILITARY COMMISSIONS IN COMPARATIVE PERSPECTIVE

Edited by Fionnuala Ní Aoláin & Oren Gross

CAMBRIDGE

CAMBRIDGE
UNIVERSITY PRESS

32 Avenue of the Americas, New York, NY 10013-2473, USA

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781107401686

First published 2013

Printed in the United States of America

A catalog record for this publication is available from the British Library.

Library of Congress Cataloging in Publication data
Guantánamo and beyond : exceptional courts and military commissions in comparative perspective / edited by Fionnuala Ní Aoláin & Oren Gross.
pages cm
Includes bibliographical references and index.
ISBN 978-1-107-00921-9 (hardback) – ISBN 978-1-107-40168-6 (pbk.)
1. Terrorism – Prevention – Law and legislation. 2. Courts of special jurisdiction.
3. Military courts. 4. Terrorism – Prevention – Law and legislation – United States.
5. Military courts – United States. I. Ní Aoláin, Fionnuala, 1967– II. Gross, Oren.
K5256.G83 2013
343'.0143–dc23 2013006439

ISBN 978-1-107-00921-9 Hardback
ISBN 978-1-107-40168-6 Paperback

Do Phádraig O' hAoláin

To Rina and Yehoshua Gross

8 Exceptional Courts in Counterterrorism

Lessons from the Foreign Intelligence Surveillance Act (FISA)

William C. Banks

THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (FISC) IS an exceptional court created by Congress to respond to a unique set of challenges related to foreign intelligence. On the one hand, U.S. presidents had on occasion authorized electronic surveillance and physical searches in pursuit of foreign intelligence without any prior judicial authorization, raising concerns that executive officials were violating the free expression and privacy rights of affected persons. On the other hand, many experts agreed that the need for speed and secrecy in collecting foreign intelligence in the face of threats of terrorism and espionage rendered traditional judicial warrant procedures ill-suited for foreign-intelligence surveillance. The FISC responded effectively to these challenges, but this exceptional court has also generated new problems. Because the factual predicate for gaining FISC approval to conduct surveillance or search is less demanding than what is required in traditional criminal cases, there has developed a considerable spillover effect, where criminal investigators and prosecutors rely on the exceptional FISC procedures to gather evidence for later use in criminal prosecutions. As a result, Fourth Amendment protections for the accused may be threatened by use of the exceptional procedures. At the same time, recent revisions to the FISC authorize the exceptional court to grant blanket approval to wholesale collection of foreign intelligence through issuance of directives to telecommunications companies and Internet service providers.

In this new role, the authorization for programmatic surveillance omits the case-by-case review of applications for surveillance and converts the FISC into an administrative clerk for executive officials.

This chapter first describes the history leading to the original creation of the FISC in 1978. Next, the role of this exceptional court in implementing the special scheme for foreign-intelligence collection is assessed, focusing on its overlap with law-enforcement objectives and the challenges of keeping up with changing technologies of surveillance and evasion. These challenges to the court's role are evaluated, as is the changing role of the FISC in the era of programmatic surveillance. In the concluding section, reforms are suggested that could help shore up the FISC in the face of the civil liberties threats posed by the continuing operation of this special court.

1. The Original FISA Scheme

Following the Watergate scandal and collapse of the Nixon presidency, congressional investigations discovered that, without seeking judicial approval, the federal government had engaged in widespread domestic surveillance for decades. The National Security Agency (NSA) had collected millions of telegrams sent from the United States abroad, and the Federal Bureau of Investigation (FBI) maintained watch lists of U.S. citizens involved in political protests. In 1976, the Senate investigatory Church Committee found that "too many people have been spied upon by too many Government agencies and [too] much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power."[1]

After the congressional investigators and media reports detailed the surveillance abuses targeting innocent civil rights and antiwar protestors in violation of their First and Fourth Amendment rights, members of

1 S. Rep. No. 94–755, AT 5 (1975).

Congress worked to devise a new law that would limit the surveillance powers of the federal law-enforcement and intelligence agencies. Although presidents had long asserted inherent authority to conduct warrantless electronic surveillance in furtherance of national security interests, congressional and White House negotiators enacted legislation that relied heavily on the unprecedented role of a new exceptional court.

Beginning in 1978, the Foreign Intelligence Surveillance Act (FISA)[2] authorized the means for electronic collection of foreign intelligence that served the nation well for many years. Before FISA, courts in the United States had extended Fourth Amendment judicial warrant requirements at two different times and in two different contexts: to government wiretapping in the law-enforcement setting in 1967; and to electronic surveillance in a case involving a domestic security investigation in 1972.[3] In the latter case, the Supreme Court rejected the government's argument that security matters are "too subtle and complex" for judicial evaluation, and the Court obliquely recommended that Congress consider regulating security investigations separately from its scheme for law enforcement, including applications to a "specially designated court."[4] The basic idea behind FISA was simple. Government may conduct intrusive electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that surveillance targets committed a crime so long as it can persuade a special Article III court – the FISC – that there exists a different kind of probable cause: reason to believe that targets of surveillance are acting on behalf of foreign powers.[5]

The FISC meets in secret, in ex parte proceedings where the targets of surveillance do not appear and have no notice of the proceedings or eventual surveillance. The court consists of eleven U.S. district court judges designated by the Chief Justice for staggered, nonrenewable terms

2 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (codified as amended in scattered titles of the U.S.C.) (hereinafter FISA).

3 *Katz v. United States*, 389 U.S. 347, 353, 358–59 (1967); *United States v. U.S. Dist. Court*, 407 U.S. 297, 313, 327 (1972).

4 407 U.S. at 320, 323.

5 FISA § 105(a) (codified at 50 U.S.C. § 1805[a] [2010]).

of up to seven years. There are no special requirements that the judges have expertise in national security or counterterrorism; all district court judges are presumptively eligible. FISA also provides for designation by the Chief Justice of three district or court of appeals judges to sit as a special court of review to hear appeals by the government from denial of an application by one of the FISC judges. The government may then appeal to the Supreme Court.

Electronic surveillance can capture movements and conversations about plans to commit a terrorist act and thus allows the government to step in before the act occurs. At the same time, electronic surveillance imposes a heavy cost in threats to personal privacy and expressive freedoms if it reaches innocent persons. Threats to civil liberties are especially acute when national security reasons are invoked to monitor political activities, as the convergence of First and Fourth Amendment values is not present in cases of ordinary crime. The government may have strong interests because of the threat of terrorism, but those targeted also have important interests to be taken into account.

FISA governed the electronic surveillance only of persons in the United States and only for the purpose of collecting foreign intelligence. It did not apply to surveillance conducted outside the United States or to foreign-to-foreign telephone communications intercepted within the United States. "Probable cause" required that a target of the surveillance be a "foreign power," an "agent of a foreign power," or since 2004, a "lone wolf" terrorism suspect – a person believed to be preparing for terrorist activities who is not shown to be affiliated with a terrorist organization. Applications to the FISC for approval of a search or surveillance had to specify "facilities" where the surveillance would be directed[6] and procedures to "minimize" the acquisition, retention, and dissemination of information not relevant to an investigation.[7]

6 *Id.* § 105(b)(1)(B).

7 *Id.* § 101(h); see also Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103–359, sec. 807, § 301(4), 108 Stat. 3423, 3443–44 (codified at 50 U.S.C. § 1821[4] [2006]) (amending FISA to include a new definition for "minimization procedures").

Before the FISC issued an order approving electronic surveillance involving a U.S. person, a FISC judge had to find probable cause that the target was an agent of a foreign power, on the basis of meeting one of four conditions: (1) the target knowingly engaged in clandestine intelligence activities on behalf of a foreign power, which "may involve" a criminal law violation; (2) the target knowingly engaged in other secret intelligence activities on behalf of a foreign power pursuant to the direction of an intelligence network, and those activities involved or were about to involve criminal law violations; (3) the target knowingly engaged in sabotage or international terrorism or was preparing for such activities; or (4) the target knowingly aided or abetted another who acted in one of the above ways.

The process undertaken by the government before going to the FISC (and before any wiretap is turned on) was elaborate and multilayered. FBI lawyers oversaw FBI agents who wanted to carry out the surveillance, and Department of Justice lawyers oversaw the FBI lawyers. Then, an application for FISA surveillance had to be approved by the Attorney General before presentation to the FISC: the department had to provide detailed information, including the identity of the target, a description of the information sought, and certifications that the information sought was believed to be foreign-intelligence information that could not reasonably be obtained by normal investigative techniques. The FISC may grant orders approving electronic surveillance anywhere within the United States.

However, what most of us think of as the judicial role in authorizing surveillance was limited by Congress in FISA in several important respects. From the beginning, FISA has allowed warrantless surveillance of non-U.S. persons for as long as one year, and another provision authorized electronic surveillance without judicial approval in an emergency situation.[8] The special court's review of FISA applications is also limited. Unlike deciding the reasonableness of surveillance in a criminal case, or

8 50 U.S.C. §§1802(a)(1),1805(e) (2010).

compliance with probable cause standards, FISC judges simply certify that a purpose of the surveillance is to collect foreign intelligence. The FISC does not determine whether there is probable cause that the electronic surveillance will result in acquisition of foreign intelligence, even where the principal objective of government investigators is to build a case for prosecution. In essence, the FISC decides that the government's paperwork is complete and in order. The legal standard requires only that the FISC find that the government certifications are not clearly erroneous.[9]

Once the statutory findings are made by the FISC, it must issue the surveillance order. The order must describe the target, the information sought, and the means of acquiring the information. The order must also determine that the government has set *minimization procedures* – mechanisms to assure that collected information is not stored or disseminated beyond the scope of what the FISC approved. The order must also set a period of time during which the surveillance may occur. The government may apply to renew the order on the same basis as the original application, and following the same procedures. More than 20,000 applications for surveillance or searches have been approved by the FISC since 1979. Less than 1 percent have been denied, and most of those denied applications were later approved after revision of the application.

To some observers, the FISC serves as a rubber stamp for executive branch officials who lack the traditional probable cause required by a magistrate in criminal cases. Some counter that the FISC is an unnecessary impediment as the executive branch strives to become nimble in collecting necessary intelligence. To others, the FISC has been a neutral arbiter necessary to ensure government accountability and legitimacy in furtherance of the narrow objectives for collecting foreign intelligence prescribed by FISA. At a minimum, the FISC provides assurances to Congress and the public that the government is meeting its statutory

9 *Id.* §1805(a).

obligations before undertaking surveillance of suspected terrorists or foreign agents.

Although the FISA scheme was complex, the legislation struck a fundamental balance. Those who worried most about the abuses of past presidents and their subordinates took comfort in the regulation of foreign-intelligence surveillance that involved Article III judges, albeit to a limited extent. The secrecy, ex parte proceedings, and corresponding lack of notice to targets was troubling, but at least applicable procedures had been prescribed by law. From the executive branch and intelligence investigators' perspectives, what was done in the past on the basis of supposed inherent constitutional authority was now subject to rules imposed by Congress. The rules lent legitimacy to secret surveillance.

The process worked well for several years as a mechanism to regulate surveillance of known intelligence targets. The FISA process and its eventual orders were always limited in two respects, however. First, whereas FISA demanded that "the purpose" of any surveillance or search be the gathering of foreign intelligence, a FISC judge in each case granted approval of the surveillance or search and found its primary purpose to be the pursuit of foreign intelligence or foreign counterintelligence information. In other words, although judicial review of FISC orders was limited, the reviewing courts used the discretion possessed by all Article III judges to require that collection of foreign intelligence was the primary purpose of the FISA investigation. Moreover, FISA was concerned with acquisition of information, not with the uses government might have for that which was collected. Second, FISA assumed that officials knew where the target was and what facilities the target would use for his communications. FISA did not authorize intelligence collection for the purpose of identifying the targets of surveillance, or of collecting aggregate communications traffic and then identifying the surveillance target. In other words, FISA envisioned case-specific surveillance with prior review by the special court, not a generic surveillance operation, and its approval architecture was accordingly geared to specific, narrowly targeted applications. FISA also recognized that persons lawfully in the

United States have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance.

Although the volume of FISA applications increased gradually through the 1990s, after 9/11 the pace of electronic intelligence collection quickened. Bush administration officials argued that traditional FISA procedures interfered with necessary "speed and agility."[10] As the pre-9/11 annual FISA applications doubled to more than 2,000 a few years later, the Director of National Intelligence (DNI) complained that more than "200 man hours" were required to prepare an application "for one [phone] number."[11] The system was, it seemed, grinding along, but it was carrying a lot of weight.

2. Challenges to the FISA System

In the years after 9/11, the FISA scheme and the role of the special court were stretched well beyond their case-specific focus on gathering foreign intelligence. Two developments placed special stresses on the FISC. Increasingly, terrorism-related activities had been criminalized, leading to frequent intersections of law enforcement and intelligence investigations. The FISC became the favored venue for seeking authorization to conduct surveillance in anticipation of prosecution in terrorism cases. As a result, the traditional law-enforcement warrant was often bypassed, and attendant Fourth Amendment interests of the targets and those on the other end of the phone line were compromised through incidental collection of communications. Second, digital communications technologies were at once exploited by foreign agents and suspected terrorists and relied on by government. The development of data-mining techniques for

10 Administration Defends NSA Eavesdropping to Congress, CNN.COM (Dec. 23, 2005), retrieved from http://articles.cnn.com/2005-12-23/politics/justice.nsa_1_security-and-privacy-national-security-agency-letter%_s=PM:POLITICS (last visited Mar. 29, 2012).

11 Chris Roberts, Transcript: Debate on the Foreign Intelligence Surveillance Act, EL PASO TIMES (Aug. 22, 2007, 1:05AM), retrieved from http://www.elpasotimes.com/news/ci_6685679 (last visited Mar. 29, 2012).

use by the government enabled investigators to depersonalize electronic surveillance and focus on gathering massive quantities of communications data to mine for further indications of terrorist activities.

Meanwhile, the Bush Administration decided to obtain what it viewed as the necessary speed and agility by tasking the NSA to undertake a massive electronic surveillance program on its own, in secret, and without involvement of FISA processes or the FISC. Within weeks of 9/11, although not reported until the December 2005 publication of an article in *The New York Times*,[12] the NSA began intercepting communications where one party was located outside the United States and the other party inside the United States. The collection occurred without gaining orders from the FISC. Instead of seeking new investigative authorities from Congress, the Bush administration simply ignored the requirements of FISA. The White House vigorously defended what it called the Terrorist Surveillance Program (TSP) after the story broke, but its legal arguments were weak and unpersuasive. Although details of the TSP remain secret, the NSA apparently would sweep up large quantities of data and then sift through it using data-mining processes. If the sifting produced information about specific individuals or groups that could be targeted for further surveillance, the NSA would then approach the FISC with a traditional FISA application.

Through statutory amendments to FISA since the September 11 attacks – in the 2001 USA Patriot Act, the 2007 Protect America Act, and the 2008 FISA Amendments Act (FAA) – the executive branch and Congress have tasked the FISC to endorse government efforts to build criminal prosecutions without following traditional Fourth Amendment rules, and to permit sweeping programmatic surveillance orders without review of the individual facts of potential targets. Even before the September 11 attacks, the United States moved to criminalize more terrorism-related activities. Although FISA and the FISC were designed

12 James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, NY TIMES, Dec. 16, 2005, at A1.

as preventives – to help the government forestall terrorism and espionage by learning about it in advance – increasingly, the investigations for foreign-intelligence and law-enforcement purposes had begun to blend and their objectives merge. Meanwhile, the FISA Court of Review approved executive branch practices that might sacrifice Fourth Amendment values and threaten the independence and legitimacy of the FISC. In the USA Patriot Act, Congress amended FISA to dismantle the wall between law enforcement and intelligence investigations by permitting the use of FISA procedures when there is "a significant" foreign-intelligence purpose to an investigation designed at the outset to build a criminal case. In other words, instead of coming to the FISC only when the primary purpose is collecting foreign intelligence, the government could launch its law-enforcement investigation with the FISC so long as some significant foreign intelligence could be collected. After the FISC objected to new Justice Department guidelines that dismantled the wall on the basis of the statutory change, the FISA Court of Review overturned the FISC and ruled that the Criminal Division of the Department of Justice could submit an application to the FISC so long as there was some significant foreign intelligence that could be collected. As a result, the role of the FISC diminished. The Court no longer questions the dominant prosecution objectives of government investigators who come before it, so long as there is some foreign-intelligence objective connected to the investigation. Similarly, its role in the new era of programmatic surveillance – to be described – is simply to approve and then occasionally monitor the suspicionless targeting procedures developed by the investigators.

3. Programmatic Surveillance and the Special Court

Under FISA as amended by the temporary Protect America Act in 2007 and the FAA in 2008, a significant portion of the FISC role has been transformed into performing a clerking function for the executive branch. Before Congress and in the context of the secret NSA

surveillance program, the Bush administration successfully emphasized the need to amend FISA to account for changes in technology and thus enable it to conduct surveillance of foreign digital communications from within the United States. But providing statutory access to U.S. digital telecommunications switches would enable NSA to access e-mail traffic traveling to or from U.S. servers, opening up a vast swath of U.S. person communications for government scrutiny. In effect, the FAA authorized the TSP. The FISA architecture was changed to accomplish this neat trick in a simple way. The definition of electronic surveillance was amended so as not to apply to surveillance of a person reasonably believed to be outside the United States. Under the new legislation, the DNI and the Attorney General were authorized to collect foreign intelligence "directed at" persons reasonably believed to be outside the United States, without obtaining an order from the FISC, even if one party to the communication was a U.S. citizen inside the United States. The predicate for collection thus became the location of the target, not his status in relation to a foreign power or terrorist organization.

Under the FAA, the role of the FISC is narrowly circumscribed. The Attorney General submits procedures to the FISC by which the government will determine that acquisitions conducted under the program meet the program targeting objectives and satisfy traditional FISA minimization procedures. After a FISC judge approves the program targeting procedures, executive branch officials authorize the surveillance of persons reasonably believed to be outside the United States and issue directives compelling communications carriers to assist. Although details of the implementation of the program authorized by the FAA remain classified, a best guess is the government uses a broad vacuum cleaner-like first stage of collection focusing on transactional data in which wholesale interception occurs following the development and implementation of filtering criteria. Targeting might be directed at a terrorist organization or telephone number or e-mail address. Then NSA engages in a more particularized collection of content after analyzing mined data.

Although traditional FISA orders are still required for "intentional acquisition" of domestic communications, and they are also required for the first time for a U.S. person targeted as a foreign power or agent of a foreign power outside the United States, accidental or incidental acquisition of communications of U.S. persons inside the United States surely occurs, especially in light of the difficulty of ascertaining a target's location. Following a periodic review of the directives issued after enactment of the FAA, the Justice Department and DNI reported to the FISC in April 2009 that the NSA had been engaging in significant and systematic over-collection of the domestic e-mail messages of Americans. After investigations had been launched, intelligence officials told *The New York Times* that the NSA exceeded its statutory authority in implementing eight to ten separate orders issued by the FISC since enactment of the FAA. Because each order could permit collection of hundreds or thousands of phone numbers or e-mail addresses, millions of individual communications could have been intercepted, including some by U.S. persons inside the United States.[13]

The FISC must approve an order for programmatic surveillance if it finds that the government's certification "contains all the required elements" and the targeting and minimization procedures are consistent with the act and the Fourth Amendment. If the FISC does not grant the government's request for an order, it may appeal to the FISA Court of Review. Once the government's request is approved, the FISC does not supervise implementation of the targeting. The FISC does conduct a semiannual review of the programmatic surveillance it has authorized.

Beyond the risks of incidental collection, many Americans feared what the government might do with the information it gathered. The FAA requires that the Attorney General and the DNI certify that minimization procedures have been or will be submitted for approval to the FISC

13 Eric Lichtblau and James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, NY TIMES, Apr. 6, 2009, at A1; James Risen and Eric Licthtblau, *Extent of E-mail Surveillance Renews Concerns in Congress*, NY TIMES, June 17, 2009, at A1.

prior to, or within seven days following, implementation.[14] However, the generic FISA minimization requirements were not modified in the FAA to accommodate the surveillance of individual targets through programmatic surveillance.[15] The FISC does not review the implementation of minimization procedures or practices for the programmatic surveillance it approves. Nor do statutory minimization rules require the government to discard communications of U.S. persons incidentally collected when the government is targeting someone abroad. The amended FISA permits the government to retain and disseminate information relating to U.S. persons so long as the government determines that it is "foreign intelligence information."[16] By implication, the government may compile databases containing foreign-intelligence information from or about U.S. persons, retain the information indefinitely, and then search the databases for information about specific U.S. persons. The combination of the government's use of the foreign-intelligence trump card to hold or disseminate information and the lack of judicial oversight of how private communications are filtered out leaves the minimization mechanism short of meeting its goals for programmatic FISA surveillance.

Although traditional FISA applications and orders may not comply with the Warrant Clause or traditional probable cause requirements, the substitution of individualized FISC review of applications and a specialized foreign intelligence-related probable cause have been construed by nearly every court that has considered their constitutionality as adequate for Fourth Amendment purposes. The programmatic orders are so dramatically different from the thirty-year FISA experience, however, that their suspicionless targeting procedures deliver us nowhere near meeting warrant or probable cause standards. Nor are the procedures reasonable

14 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, § 702, 122 Stat. 2436 (codified at 50 U.S.C. § 1881a[3] [2008]).

15 *Id.*

16 50 U.S.C. § 1821(4)(B) (indicating that nonpublicly available information can be disseminated in a manner that identifies a U.S. person without their consent when such person's identity "is necessary to understand such foreign intelligence information or assess its importance").

in Fourth Amendment terms. Nor are any of the administrative officials required to find that the program targets are foreign agents, have or will engage in criminal activity, or are connected in any way with terrorism.

The programmatic title of FISA subordinates the FISC to the discretionary decisions of the Justice Department. Every FAA decision bearing on specific intelligence targets – except for the required FISC finding that a U.S. person outside the United States targeted for surveillance is a foreign power or agent of a foreign power – is made by executive branch officials and is not subject to review by the FISC or another judge. Prior identification of targets to a judge protects innocent third parties from being swept up in the surveillance and enforces the hallmark predicate for government surveillance – individualized suspicion. By focusing on what the collected information may be used for, FISA and the FISC (until the FAA) provided a useful, albeit opaque, mechanism to ensure the accountability of the collection scheme.

4. Shoring up the FISC as an Exceptional Court

The combined stresses of criminalizing terrorist activities and the digital revolution in communication and surveillance technologies have transformed the FISC from an effective model for an exceptional court that works into a clerk for executive branch investigators. Instead of doing what judges are good at – sifting facts and applying them to legal standards – the FISC spends much of its collective time on ministerial tasks. Unless reforms are made the special court may lose its independence and, over time, its legitimacy.

The original FISA procedure for reviewing applications for surveillance of foreign agents and lone wolves has served the nation well as a secondary, specialized system that serves discrete and important objectives. But the FISA experience shows in vivid ways the dangers that occur when a secondary system and its standards are mingled with those from the primary federal system, in this instance law enforcement and criminal prosecution in the federal courts. The byproduct of mingling the two is

that the constitutional protections embedded in federal court prosecution are watered down and gradually eviscerated. Without FISA and the FISC, the federal courts would not have authorized electronic surveillance and physical searches absent probable cause of criminal activities or, in the event of exigent circumstances, on the basis of a finding of reasonableness. Employing the FISC, the government makes a less burdensome showing to the judge, and the target is never given notice of the application or the eventual surveillance. As ever more prosecutions related to terrorism are launched on the strength of FISA surveillance, the federal courts review the surveillance subject to permission already granted to the FISC by Congress. The courts do not undertake a de novo review of the surveillance application.

Because so many terrorism-related crimes now populate the criminal code in the United States it is unrealistic to expect any version of the wall that used to separate law enforcement and intelligence investigations to be rebuilt. The blending of the criminal and foreign-intelligence functions and personnel in the Justice Department, however, calls for reforms to protect the independence of the FISC and the integrity of the FISA process. One partial fix would be to create adversarial roles and processes. Both traditional FISA applications and certifications for programmatic surveillance orders are created, reviewed, critiqued, and presented entirely by Justice Department personnel, all with a singular objective to gain FISC approval of the applications and certifications. Congress or the FISC could create a straw adversary within the Justice Department to represent the interests of the described targets in an application or those likely affected by programmatic surveillance. The FISC could also be authorized by Congress to appoint cleared counsel to appear in connection with selected applications. Publicly released FISA Court of Review decisions demonstrate the shortcomings of insufficient procedures for those opposed to the government position to participate in the appeals process. Even where security concerns may require closing an argument or other session before the Court in part, an open session for cleared counsel to present arguments in opposition to the

government would assist the FISC or FISA Court of Review in weighing legal arguments and enhance the legitimacy of the otherwise secret process in the eyes of the public.

Congress did not modify the traditional minimization requirements in FISA when it approved programmatic surveillance, and it is surely possible that extensive personal communications of innocent Americans will be retained in government databases for the foreseeable future. It would be possible for the FISC to make rules detailing specific minimization procedures in connection with programmatic orders. With the wall down and basket warrants enabling government access to vast stores of personal records, new rules protecting against abuses in retaining and misusing personal information would help restore confidence in the FISA system. As an Article III court, the FISC likely has authority to so regulate on its own, analogous to the role courts have played in defining other federal judicial rules.

One persistent problem with exceptional courts concerns their expertise. Courts such as the FISC are created to manage a highly secretive and factually nuanced system of surveillance, but the Article III judges eligible for the FISC have no special training in national security surveillance. Although some of those appointed to the FISC have had relevant military experience or have written scholarly articles on electronic surveillance, the FISC judges are not typically expert on the questions they are asked to review. Moreover, FISA itself seriously truncates the judicial role throughout the FISA processes. By and large, the FISC signs off on certifications from the government that collection of foreign intelligence is a significant purpose of the action at issue. The judges find probable cause, but only regarding the target's status as a foreign power, a foreign power's agent, or a lone wolf, and that the facilities targeted are used by the target. The FISC does not assess in any respect whether the approved surveillance will result in acquisition of the foreign intelligence sought. In effect, the FISC is a record keeper – is the government's paper application in order? Under the act as amended for programmatic surveillance, the FISC does even less in measuring the government's application for

surveillance to a factual predicate. Instead of probable cause of foreign agency, for example, the FISC only determines that the target is or targets are reasonably believed to be outside the United States.

In programmatic surveillance the FISC may reject a certification only if does not "contain all the required elements," or the procedures "are not consistent with the requirements" of the act. The FAA does build in audits by inspectors general, and it provides for sharing some reporting information with congressional committees. The FISC, too, may review the programmatic surveillance procedures subject to "the need of the United States to obtain, produce, and disseminate foreign-intelligence information."[17]

Although the Supreme Court has not decided a FISA case – either on judicial review of a criminal conviction or a challenge to the FISC or its processes – all the lower courts that have heard challenges to the FISA architecture have upheld the scheme. The absence of adversarial proceedings and the use of ex parte processes do not violate the Article III case or controversy requirements, according to reviewing courts. Nor are challenges to FISA orders barred by the political question doctrine. As for substantive complaints, reviewing courts have found that FISA does not violate the Fourth Amendment, the Fifth Amendment's Confrontation Clause, or the First Amendment's free expression protections.[18]

Conclusions

The FISC remains an especially successful exceptional court. It was created to do a job that traditional Article III judges were reluctant to do and that the executive branch preferred be left to them. At the same time, the FISC was created at a time when surveillance abuses cast a shadow over the integrity of these important foreign-intelligence activities. In the years between creation of the court and the 9/11 attacks, the FISC

17 *Id.* § 1821(4)(A) (2010).

18 But see *Mayfield v. United States*, 504 F. Supp. 2d 1023 (D. Or. 2007) (finding Fourth Amendment violation), rev'd, 588 F. 3d 1252 (9th Cir. 2009).

developed some expertise in foreign-intelligence surveillance and the court gained considerable respect from observers inside and outside government. Although the secrecy of the FISC and its processes produced a measure of skepticism about what the court actually did behind closed doors, reviewing courts and others that followed the surveillance activities closely were assured that the FISC approved electronic surveillance only when its primary purpose was the collection of foreign intelligence.

The combination of the criminalization of many terrorist activities and the digital revolution in communications and surveillance capabilities altered the role of the FISC and, following the 2008 amendments to FISA, strained its credibility as an independent arbiter of lawful FISA surveillance. The use of FISA processes to build criminal cases is regrettable, in my view, but the lowering of the wall between law enforcement and intelligence-gathering has been supported by the FISA Court of Review and there is considerable momentum behind the use of FISA in building criminal cases. The programmatic surveillance now sanctioned by the FISC is more problematic, however, because the special court has assumed more of a clerical function than a judicial role. There remain opportunities to revise minimization rules, either through new legislation or FISC rulemaking, and to make government retention or dissemination of private information about innocent persons less likely. At the same time, if we must tolerate sweeping digital collection of our personal data, the FISC should have greater and more meaningful opportunities to oversee its collection – if not in advance, then after the fact.

Part II EXCEPTIONAL COURTS AND MILITARY COMMISSIONS ELSEWHERE