**The Ear of Dionysus:**
*Rethinking Foreign Intelligence Surveillance*

9 YALE J. L. & TECH. (forthcoming Spring 2007)  

K. A. Taipale *

A précis of this article was published as *Rethinking Foreign Intelligence Surveillance* in  
WORLD POLICY JOURNAL Vol. XIII No. 4 (Winter 2006-2007)

---

**Introduction.**

As the 110th Congress begins to flex its atrophied oversight muscle † it bears reminding in the ongoing debate over who should have the authority to authorize and oversight foreign intelligence surveillance programs, ‡ that someone must, § and the existing mechanisms,

---

† See, e.g., Donna Leinwand, Senate grills Gonzales over spying, USA TODAY (Jan 19, 2007); Lara Jakes Jordan, Senators Grill Gonzales Over Spy Program, SAN FRAN. CHRON. (Jan. 19, 2007); Tom Brune, Senate Judiciary Committee questions surveillance, NEWSDAY (Jan. 18, 2007); Jeff Bliss, Rockefeller Says He May Subpoena Documents on Spying, Bloomberg News (Jan. 26, 2007). See generally Brian Knowlton, Top Democrat seeks wider NSA hearings, INT’L HERALD TRIB. (Jan. 1, 2007); Shaun Waterman, Dems Take Over Hill Intel Panels, UPI (Dec. 8, 2006) (“Democrats say … they will launch a vigorous push for oversight of some of the most secret and controversial programs … employed in the war on terror”); Eric Lichtblau, With Power Set to Be Split, Wiretaps Re-emerge as Issue, N.Y. TIMES (Nov. 10, 2006) (“Democrats … vowed to investigate the [National Security Agency Terrorist Surveillance Program] aggressively once they assume power”).

‡ This public debate has taken place within the context of media disclosures regarding certain classified operational programs of the National Security Agency (“NSA”), including the Terrorist Surveillance Program (“TSP”) in which certain international calls of suspected terrorists were being monitored pursuant to Presidential authority without warrants in circumstances that otherwise might implicate the warrant requirements of the Foreign Intelligence Surveillance Act of 1978 (“FISA”) (see James Risen & Eric Lichtblau, Bush Lets U.S. Spy on Callers Without Courts, N.Y. TIMES, Dec. 16, 2005) and an alleged program to collect and analyze Call Detail Records (CDRs) from U.S. telecommunication carriers (see Leslie Cauley, NSA has massive database of Americans’ phone calls, USA TODAY, May 11, 2006). On January 17, 2007, Attorney General Alberto Gonzales informed the chairman and ranking member of the U.S. Senate Committee on the Judiciary by letter that the Foreign Intelligence Surveillance Court (“FISC”) had issued orders authorizing certain surveillance previously authorized under the NSA TSP. The letter stated that as a result of these orders, "any electronic surveillance that was [previously] occurring as part of the [TSP] will now be conducted subject to the approval of the [FISC]” and, accordingly, that “the President has determined not to reauthorize the [program] when the current authorization expires.” For the reasons outlined in this article, FISA should be amended to provide an explicit statutory basis for these orders to address the problems outlined herein.
in particular, the Foreign Intelligence Surveillance Act of 1978 ("FISA") ⁴ and its related procedures, are no longer adequate and must be updated. The FISA simply did not anticipate the nature of the current threat to national security from transnational terrorism, nor did it anticipate the development of global communication networks or advanced technical methods for intelligence gathering. ⁵

New technologies do not determine human fates but they do alter the spectrum of potentialities within which people act. ⁶ This article examines how technology and certain related developments have enabled new threats and new response mechanisms that challenge existing policy constructs and legal procedures in the context of foreign intelligence surveillance. ⁷ This article does not argue that these developments justify abandoning long-held bedrock principles of democratic liberty—nor even that some new "balance" between security and liberty need be achieved ⁸ —rather, it argues that familiar, existing oversight and control mechanisms—including FISA—or their

---

³ See Knowlton, supra note 1 ("[Senator] Schumer said the problem was not with good-faith efforts to make Americans secure—no Democrat opposed that, he said—but with the president's authority to do so unilaterally.")


⁵ In general, FISA was intended to warrant electronic surveillance where there is probable cause to believe the target is an “agent of a foreign power,” §1805, thus, is useful for monitoring known agents of an enemy power. FISA did attempt to address the then nascent threat of international terrorism by defining “foreign power” to include “groups engaged in international terrorism” for purposes of the statute, §1801(a)(4), and, in 2003, the definition was expanded to include so-called “lone wolves”. However, for reasons outlined in Section I of this article, the nature of the current terrorist threat does not easily conform to “agent of a foreign power” equivalence for these purposes and FISA provides no mechanisms for using advanced technical methods to help identify such agents in the first place.


⁷ It is beyond the scope of this article to address how these developments affect other national security and law enforcement policy, or to address the underlying philosophical or political issues regarding appropriate social-control mechanisms more generally. However, these developments take place within an ongoing transformation of modern societies from a notional Beccarian model of criminal justice based on accountability for deviant actions after they occur, see generally Cesare Beccaria, On Crimes and Punishment (1764), to a Foucauldian model based on authorization, preemption, and general social compliance through ubiquitous preventative surveillance and control through system constraints. See generally Michel Foucault, Discipline and Punish (1975, Alan Sheridan, tr., 1977, 1995). In this emergent model, ‘security’ is geared not towards traditional policing through arrest and prosecution but to risk management through surveillance, exchange of information, auditing, communication, and classification. See generally The New Politics of Surveillance and Visibility (Kevin D. Haggarty & Richard V. Ericson, eds., 2006) (discussing the collection and analysis of information for social-control).

⁸ Indeed, I have argued elsewhere that the very notion of balance is misleading and deflects the discourse since implicit in the use of balance as metaphor is that some fulcrum point exists at which the correct amount of security and liberty can be achieved. However, liberty and security are not dichotomous rivals to be traded one for the other in some zero sum game but rather each vital interests to be reconciled, and, thus, dual obligations to be met. See, e.g., K. A. Taipale, Introduction to Domestic Security and Civil Liberties in The McGraw-Hill Homeland Security Handbook 1009-1012 (David Kamien, ed., 2006); K. A. Taipale, Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd, 7 YALE J. L. & TECH. 123 at 127; 9 INT'L. J. COMM. L. & POL'Y 8 (Dec. 2004) (hereinafter, "Frankenstein").
analyses can be applied in these novel, technologically-enabled circumstances, but only if the challenges and opportunities are better understood and the laws and procedures are updated to accommodate needed change.

This article is intended neither as critique nor endorsement of any particular government surveillance program or action; rather, it attempts to highlight certain issues critical to a reasoned debate and democratic resolution of these issues. This article also does not address directly whether the President currently has inherent or statutory authority to approve any specific operational program nor whether press disclosure of classified government programs is appropriate or justified.

---

9 In particular, neither of the classified programs referred to in note 2 supra.

10 Whether the President has inherent or statutory authority to authorize foreign intelligence surveillance programs, including the TSP, is currently being litigated in ACLU v. NSA, No. 06-CV-10204 (E.D. Mich. filed Jan. 17, 2006); Center for Constitutional Rights v. Bush, No. 06-CV-00313 (S.D. N.Y. filed Jan 17, 2006); and Hepting v. AT&T No. C-06-0672-JCS (N.D. Ca. filed Jan 31, 2006) (class action suit against AT&T and other telecommunications providers for participating in the NSA surveillance programs).

On Aug. 17, 2006, the District Court in ACLU v. NSA ruled that the TSP was illegal under FISA and unconstitutional under the First and Fourth Amendments. That opinion has been heavily criticized. See, e.g., Jack Balkin, Federal court strikes down NSA domestic surveillance program, Balkinization (Aug. 17, 2006) available at http://balkin.blogspot.com/2006/08/federal-court-strikes-down-nsa.html (“much of the opinion is disappointing, and … a bit confused”); Editorial, A Judicial Misfire, WASH. POST (Aug. 18, 2006) (The decision “is neither careful nor scholarly” and “as a piece of judicial work—that is, as a guide to what the law requires and how it either restrains or permits the NSA's program—[the] opinion will not be helpful”). On Oct. 4, 2006, a unanimous three-judge panel of the United States Court of Appeals for the Sixth Circuit stayed the District Court's ruling while the government's appeal is considered. On Jan. 24, 2007 the Justice Department asked that the case be dismissed as moot. See Dan Eggen, Dismissal of Lawsuit Against Warrantless Wiretaps Sought, WASH. POST (Jan. 25, 2007) (“A lawsuit challenging the legality of the National Security Agency's warrantless surveillance program should be thrown out because the government is now conducting the wiretaps under the authority of a secret intelligence court, according to court papers filed by the Justice Department yesterday”). See Government’s Supplemental Submission Discussing the Implications of the Intervening FISA Court Orders of Jan. 10, 2007 at 8-15, ACLU v. NSA (No. 06-CV-10204) (submission filed Jan 24, 2007). On Jan. 31, 2007 a three-judge panel of the Sixth Circuit Court of Appeals heard oral arguments on these issues. See Adam Liptak, Judges Weigh Arguments In U.S. Eavesdropping Case, N.Y. TIMES (Feb. 1, 2007).

The understanding that the President retains some Constitutional power to conduct surveillance beyond FISA despite the “exclusivity” provision set forth in 18 U.S.C. §2511(2)(f) (“...procedures in … the [FISA] shall be the exclusive means by which [foreign intelligence] electronic surveillance … may be conducted”), is evidenced in part by the Congressional testimony of President Gerald Ford’s Attorney General Edward Levi (there is “a presidential [surveillance] power which cannot be limited, no matter what Congress says”) and President Jimmy Carter’s Attorney General Griffin Bell (FISA “does not take away the power of the president under the Constitution”) at the time that FISA was negotiated and enacted. See John Schmidt, When Terrorists Talk ..., LEGAL TIMES (Sep. 18, 2006) (discussing the exclusivity provision of FISA and the President’s inherent surveillance power). “[Levi warned] that the unpredictability of foreign threats to the nation and the likelihood of ongoing changes in communication technologies made it ‘extraordinarily dangerous’ to … not acknowledge the president’s retained surveillance power” Id. (emphasis added).

11 For example, on Jun. 23, 2006, the N.Y. Times disclosed another secret program that allegedly “trac[ed] transactions of people suspected of having ties to Al Qaeda by reviewing records [of wire transfers] from [the Society for Worldwide Interbank Financial Telecommunication (“Swift”)] … a Belgian cooperative that routes about $6 trillion daily between banks, brokerages, stock exchanges and other
This article is organized into five parts: this Introduction, three descriptive sections, and a brief Conclusion. Section I: Changing Base Conditions describes the changing nature of the threat, the shift to preemptive strategies in response, and the need for surveillance to support preemption; Section II: The Ear of Dionysus briefly describes the nature of modern communication networks and certain related technology developments, and examines how three situations—transit intercepts, collateral intercepts, and automated monitoring—cannot be accommodated by FISA as currently constituted; and, Section III: Fixing Foreign Intelligence Surveillance suggests some potential solutions that preserve existing Fourth Amendment principles and protections while still addressing these failures. Finally, the Conclusion reiterates the need to get beyond backward looking recriminations and to craft progressive consensual solutions.

**Section I: Changing Base Conditions.**

Both security and liberty today function within a changing technological context; but mere recognition of changed circumstance itself is not sufficiently determinative of desirable outcomes. It is acceptable neither to say that ‘everything changed on 9/11’ and thus we must accept lessened liberty, nor to say that we have ‘faced greater threats before’ and thus we should cling to outmoded praxis developed at another time, to deal with a different threat. Rather, changing context requires reflective reexamination of institutions.” Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES (Jun. 23, 2006). The article alleged no illegalities or abuses and noted that a White House spokesperson reported “[t]he president is concerned that once again The New York Times has chosen to expose a classified program that is working to protect our citizens.” Subsequently, the N.Y. Times Public Editor Byron Calame published a mea culpa in which he wrote “I don’t think the [Swift] article should have been published” because the program was clearly legal under U.S. law and there were no allegations that any information had been misused. Byron Calame, *Banking data: A Mea Culpa*, N.Y. TIMES (Oct. 22, 2006). However, according to House Intelligence Committee Chairman Pete Hoekstra, “The mea culpa of the N.Y. Times public editor comes too late to stop the damage done to one of our nation’s leading tools to track, understand and prevent the money transfers that enable terrorist attacks.” Press Release, *Hoekstra Statement on New York Times Mea Culpa* (Oct. 25, 2006) available at http://hoekstra.house.gov/News/DocumentSingle.aspx?DocumentID=51935; see also Editorial, *Not So Swift*, WASH. TIMES (Oct. 24, 2006) (“The [N.Y.] Times never adequately defended its exposure of the program … if no illegality or immoral action has taken place, and there is a very high risk of genuinely endangering national security, the decision must be against publication … sometimes the media simply needs to let government do its job”).

For a discussion of whether The New York Times violated the Espionage Act, 18 U.S.C. § 798 (Disclosure of classified information), when it disclosed the TSP, see Gabriel Schoenfeld, *Has the “New York Times” Violated the Espionage Act?* COMMENTARY (March 2006) (“The real question … is whether … we as a nation can afford to permit the reporters and editors of [the New York Times] to become the unelected authority that determines for all of us what is a legitimate secret and what is not. … The laws governing [the disclosure of the TSP by the Times] are perfectly clear, will they be enforced?” Id. at 31)

For example, it is particularly delusive to believe that because we successfully faced a greater destructive threat from the Soviet Union that we can also successfully meet the current threat with the same outdated strategies or tools, that is, without adapting to change. It is the qualitative nature of the current threat, not just its quantitative force that needs to be considered in devising successful counterstrategies. For example, accountability strategies useful for countering nation state adversaries—for example, pursuing nuclear deterrence through a doctrine of mutual assured destruction (MAD)—must be recognized as ineffective against attackers unconstrained by after-the-fact punishment, in particular, suicide attackers...
previously satisfactory practices based on an informed appreciation of the complex interactions of new threats with new opportunities, and with a willingness to reconstruct outmoded habitudes. While we simply cannot abandon cherished values because maintaining them is difficult, neither can we simply resist change because it is uncomforting.

The Changing Nature of the Threat and the Shift to Preemption

Enabled in part by force-multiplying technologies, the potential to initiate catastrophic outcomes to national security is devolving from other nation states (the traditional target of national security power) to organized but stateless groups (the traditional target of law enforcement power) blurring the previously clear demarcation between reactive law enforcement policies and preemptive national security strategies. Organized groups of non-state actors now have the potential capacity and capability to inflict the kind of destructive outcomes that can threaten national survival by undermining the public confidence that maintains the economic and political systems in modern Western democracies. In simple terms, the threat to national security is no longer confined only to other nation states. As Thomas Friedman writes in The World is Flat, 21st century terrorism is the globalization of 20th century terrorism.

without accountable patrons or other support infrastructure subject to sanction or retaliation. So, too, law enforcement strategies developed to deal with organized crime or other economically motivated conspiracies like drug smuggling are inadequate when employed against ideologically motivated forces.


Technologically-enabled capacities include the use of so-called weapons of mass destruction (WMDs), including chemical, nuclear, and biological (CNB) weapons, the use of airliners or other advanced technology infrastructure as a weapon system, or the targeting of technological vulnerabilities, for example, critical infrastructure control systems (SCADA). See, e.g., Alan Joch, Terrorists brandish tech sword, too, FEDERAL COMPUTER WEEK (Aug. 28, 2006).

Technologically-enabled capabilities include recruitment, organization, funding, planning, training, targeting, and command-and-control using global communication networks and the Internet. See, e.g., Joch, supra note 14.

In addition to the approximately 3,000 immediate deaths resulting from the terrorist attack on the World Trade Center towers and Pentagon, the attack has been variously estimated to have caused between $50 billion and $100 billion in direct economic loss. Estimates of indirect losses in the immediate aftermath exceeded $500 billion nationwide. General Accounting Office U.S. Congress, GAO-02-700R, Review of Studies of the Economic Impact of the September 11, 2001 Terrorist Attacks on the World Trade Center (2002). In the eighteen months following the attacks 2.5 million jobs were estimated to have been lost in the U.S. Brian Sullivan, Job losses since 9/11 attacks top 2.5 million, COMPUTERWORLD (Mar. 25, 2003). The total cost of knock-on effects, including the cost to national economic efficiency, competitiveness, and civil liberties from policies implemented in the response to the attacks are incalculable.

Indeed, technology is affording non-state competitors—including international terrorist groups, organized crime gangs, rogue multinational corporations, and other hostile NGOs—the potential to exercise economic, political, and military power, including violence, at a scale that has traditionally been subject to sovereign nation state monopoly and which is beyond the reach of any single nation state’s jurisdiction to
Thus, there has emerged a political consensus, at least with regard to certain threats, to take a preemptive rather than reactive approach. 19 “Terrorism cannot be treated as a reactive law enforcement issue, in which we wait until after the bad guys pull the trigger before we stop them.” 20 The policy debate, then, is not about preemption itself—even the most strident civil libertarians concede the need to identify and stop terrorists before they act 21—but instead revolves around what methods are to be properly employed in this endeavor.

The Need for Surveillance

Preemption of terrorist attacks that can occur at any place and any time requires information useful to anticipate and counter future events—that is, it requires actionable intelligence. 22 Since terrorist attacks at scales that can actually endanger national control, thus potentially undermining the entire Westphalian construct of international political relations. However, it is beyond the scope of this article to address these broader issues. See generally Martin van Creveld, THE RISE AND DECLINE OF THE STATE at 377-394 (Cambridge Univ. Press 1999) (“Technology goes international”).

18 Thomas Friedman, THE WORLD IS FLAT (2006). Globalized transnational terrorism, enabled and empowered in part by technology developments (see notes 14 and 15 supra), is simply qualitatively different than the then nascent “international terrorism” threat that was belated addressed in FISA by simply expanding the definition of “foreign power” to include “groups engaged in international terrorism.” See generally NETWORKS, TERRORISM AND GLOBAL INSURGENCY (Robert J. Bunker, ed. 2005) (assessing the threat posed by global terrorism).

19 It is beyond the scope of this article to delineate precisely where the line should be drawn between threats requiring a preemptive approach and those that remain amenable to traditional reactive law enforcement. For purposes of this article we assume that there is some threat from loosely organized global terrorist groups that implicates national security and therefore requires a preemptive approach. See, e.g., Osama Bin Laden, Declaration of War against Americans Occupying the Land of the Two Holy Places (1996); Osama Bin Laden, et al., Jihad Against the Jews and Crusaders, World Islamic Front Statement (1998). However, it is not appropriate, nor realistic, to assume that all manner of ‘terrorist’ acts are subject to preemptive strategies or are preventable. It is axiomatic that national security assets, including foreign intelligence surveillance capabilities, should be employed only against true threats to national security and not used for general law enforcement or other social-control purposes.

20 Editorial, The Limits of Hindsight, WALL ST. J. (Jul. 28, 2003) at A10. See also U.S. Department of Justice, Fact Sheet: Shifting from Prosecution to Prevention, Redesigning the Justice Department to Prevent Future Acts of Terrorism (May 29, 2002).

21 See, e.g., Statement of the Honorable Edward Kennedy, United States Senator, Committee on the Judiciary (Jan. 10, 2007) (“We all agree on the need for strong powers to investigate terrorism [and] prevent future attacks”).

22 Terrorism, by indiscriminately targeting civilians and infrastructure, limits the effectiveness of certain other counterstrategies that are otherwise useful, i.e., useful against nation state adversaries conforming to the international laws of armed conflict (LOAC). For example, an effective defensive strategy against a state adversary might include hardening military targets. However, except in specific contexts such as reinforcing and locking cockpit doors, one cannot harden all potential terrorist targets, not even the high value ones. “The nation could never sufficiently harden all potential targets of attack.” Markle Foundation, Second Report of the Markle Task Force on National Security in the Information Age: Creating a Trusted Network for Homeland Security at 1 (2003) (arguing for improved information sharing in order to identify terrorists before they act).
security generally still require some form of organization, and organization requires communication, effective counterterrorism strategies in part require the surveillance or analysis of communications to uncover evidence of organization, relationships, or other relevant indicia indicative or predictive of potential threats—that is, actionable intelligence—so that additional law enforcement or security resources can then be allocated to such threats preemptively to prevent attacks. 23

As with the notion of preemption generally, even the most strident critics of any particular surveillance practice concede the legitimate need for surveillance to monitor the communications of terrorists to stop them before they can act. 24 Again the contentious issue is what rules ought govern such surveillance—and who should have the authority to authorize it and with what oversight. Unfortunately, while FISA “retains value as a framework for monitoring the communications of known terrorists, … it is hopeless as a framework for detecting terrorists. [FISA] requires that surveillance be conducted pursuant to warrants based on probable cause to believe that the target of surveillance is a terrorist, when the desperate need is to find out who is a terrorist.” 25 “FISA was built for long-term coverage against known agents of an enemy power” but the current need is to employ technical means to help “detect and prevent” future terrorist activity. 26

The Dissolving Perimeter of Defense

The final characteristic of the current terrorist threat to be considered in this section is that the perimeter of effective defense is dissolving. The traditional “line at the border” based defense, useful against threats from other nation states, is insufficient against a parlous enemy 27 that moves easily across borders and hides among the general

23 Nation-threatening levels of destruction or disruption can generally only be achieved with highly coordinated conventional attacks, multidimensional assaults calculated to magnify the disruption, or the use of chemical, biological, or nuclear (CBN) weapons. These methods of attack are still likely to need the kind of organization that requires the use of communications for coordination of action or resource allocation thus providing opportunities for potential discovery or surveillance.

24 See, e.g., Adam Nagourney, Seeking Edge In Spy Debate, N.Y. TIMES (Jan. 23, 2006) (“We all support surveillance … .’ [Senator John] Kerry said.”); and Statement released by U.S. Senator Patrick Leahy (Feb. 15, 2006) (“We all agree that we should be wiretapping al Qaeda terrorists”).


26 Statement by Gen. Michael Hayden, White House Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005). FISA was essentially enacted to address the problem of surveillance of adversary state espionage activities and included international terrorism against national interests as an afterthought by defining “groups engaged in international terrorism” as “foreign powers” for purposes of the statute, however, it simply did not contemplate the nature or scale of a globalized, non-state group conspiracy enabled by modern technology that could directly threaten long-term national security.

population taking advantage of open societies to mask their own organization and activities. 28 Thus, arbitrary national boundary-based rules for conducting electronic surveillance—like those in FISA that are triggered by activity “within the United States” or involving “U.S. persons”—that do not conform to actual patterns of global terrorist activity (and which may have been perfectly adequate in prior contexts with known or identifiable adversaries) are deficient to deal with ambiguous threats.

As described below, these challenges are particularly acute for electronic surveillance in global communications systems where rules based on geographically-determined jurisdiction and the physical location of information infrastructure to be targeted are undermined by the global nature of the infrastructure and information flows, and rules based on indeterminate or arbitrary attributes, such as citizenship, are technically impossible to enforce. 29

Section II: The Ear of Dionysus.

The Ear of Dionysus (L’Orecchio di Dionigi) is the name given by the belligerently Baroque painter Caravaggio (1571-1610) 30 to a cave in Syracuse in which, legend has it,
Dionysus[^31] took advantage of the perfect natural acoustics that allowed eavesdropping on all conversations from one central spot.[^32] *Ear of Dionysius* has come to generically refer to any structure in which the acoustic architecture naturally allows conversations to be heard surreptitiously at a distance—so, too, then, the global communication infrastructure.

**FISA is Inadequate**

In addition to the general challenges detailed in the earlier section relating to preemption, FISA is inadequate as currently constituted in particular because it did not anticipate the development of global communication networks or advanced technical methods for intelligence gathering. Thus, it fails in practice to accommodate three specific circumstances:

- **First**, because FISA has been interpreted by some to require a warrant for any electronic surveillance that “occurs in the United States” if there is a substantial likelihood of intercepting contents of a communication “to or from a person in the United States” it unnecessarily constrains surveillance of wholly foreign communications—say a phone call between an al Qa’ida safe house in Pakistan and a known terrorist financier in Indonesia—if the interception is physically accomplished at a telecommunications switch on U.S. soil while the communication is in transit (“transit intercepts”).[^33]

- **Second**, FISA provides a cumbersome binary mechanism requiring individual application to the FISA court for authorization to target a specific U.S. person or source based on showing probable cause of a connection to a foreign power or terrorist organization prior to any electronic surveillance, even in circumstances where collateral intercepts incidental to an authorized foreign intelligence target not subject to FISA might indicate reasonable suspicion that would require follow up

[^31]: Dionysus, the bastard son of Zeus and the mortal Semele, was the mythic god of fertility, wine, intoxication, and creative ecstasy. It was Dionysus who granted Midas the golden touch, then was benignant enough to relieve him of the power when it proved inconvenient. *See generally* Robert Graves, *The Greek Myths* at 103-110, 281-282 (1960, 1955).


> One issue of concern to the [FISC] … is whether the court has legal authority over calls outside the United States that happen to pass through American-based telephonic "switches" … Now that foreign calls were being routed through switches on American soil, some judges and law enforcement officials regarded eavesdropping on those calls as a possible violation of those decades-old restrictions, including the [FISA], which requires court-approved warrants for domestic surveillance.

And see note 34 infra.
surveillance to determine whether probable cause exists (“collateral intercepts”), 34 and

• Third, FISA does not provide any mechanism for programmatic pre-approval of technical methods like automated data analysis or filtering that may be the very method necessary for uncovering the connection to a foreign terrorist organization or activity in the first place (“automated analysis”).

To understand why FISA is inadequate in these circumstances requires in part an understanding of the nature of modern communications networks.

Transit Intercepts: From circuit-based to packet-based communication networks.

Thirty years ago when FISA was being drafted it made sense to speak exclusively about the interception of a targeted communication—one in which there were

---

34 The current NSA Terrorist Surveillance Program as described in media reports does not appear to fully address the transit or collateral intercept problems raised in this article. In fact, it appears that the TSP was intended to address only a narrower procedural problem resulting from the transit intercept problem (that is, where FISA requirements are being triggered only because the interception “occurs in the U.S.”), but involving collateral intercepts of international calls of a foreign intelligence target communicating to or from the U.S.—even where such collateral intercepts may themselves amount to probable cause.

Collateral intercepts of a foreign target communicating with a person in the United States would generally not be subject to FISA if the surveillance was conducted from abroad, but would be subject to FISA requirements if the interception was conducted at a switch within the United States. See 50 U.S.C. §1801 (f): “Electronic surveillance means: … (2) the acquisition … of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, … [emphasis added].” The problem is simply that FISA requirements are now being triggered for communications that were not originally intended to be subject to FISA (that is, those incidental to a legitimate foreign target intercept) only because the capability to do foreign intercepts from within the United States is now technically feasible (and was not anticipated at the time FISA was enacted).

The untenable result is that if the NSA were lawfully targeting a foreign source communicating with someone in the United States by monitoring a foreign switch then that collateral communication would generally only be subject to minimization requirements consistent with Executive Order 12,333 and could subsequently be used in support of an application for targeting the U.S. person or source; however, if that same surveillance was being conducted at a switch in the United States, information from the collateral intercept could not be used as predicate for a FISA warrant if the original interception was deemed to have itself required a FISA warrant (because it “occurred in the U.S.”). Indeed, it appears that this specific issue was a particular concern of the FISC. See Carol D. Leonnig, Surveillance Court is Seeking Answers, WASH. POST (Jan. 5, 2006) (“[the presiding FISC judge] had … raised concerns … about the risk that the government could taint the integrity of the [FISC’s] work by using information it gained via wiretapping [pursuant to Presidential authority under the TSP] to obtain warrants … under the Foreign Intelligence Surveillance Act.”)

This problem could not simply be avoided by getting a FISA warrant for the original intercept of the call to or from the U.S. because it is uncertain whether the FISC even has (or should have) jurisdiction over the surveillance of a purely foreign target and it could not be known a priori that a communication to or from the U.S. would take place or with whom (thus, it would be impossible to meet the requirements to support a traditional FISA warrant application). But see note 44 infra discussing the FISC orders, which are believed to take the form of anticipatory warrants to authorize such intercepts.
usually two known ends and a dedicated ("circuit-based") communication channel that could be “tapped.” In modern networks, however, data and … [digital] voice communications are broken up into discrete packets that travel along independent routes between point of origin and destination where these fragments are then reassembled into the original whole message. Not only is there no longer a dedicated circuit, but individual packets from the same communication may take completely different paths to their destination.\footnote{K. A. Taipale, \textit{Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance}, N.Y.U. Rev. L. & Security, No. VII Suppl. Bull. on L. & Sec.: The NSA and the War on Terror \textit{(Spring 2006)} (hereinafter “\textit{Whispering Wires}”) at http://whisperingwires.info/.


In these “packet-based” networks, computerized switches (“routers”) determine in real time and at various points along the way the most efficient route for ongoing packet traffic to take depending on current availability and congestion on the network, not simply on the shortest distance between two points. “Such random global route selection means that the switches carrying calls from Cleveland to Chicago, for example, may also be carrying calls from Islamabad to Jakarta.”\footnote{James Risen, \textit{State of War: The Secret History of the CIA and the Bush Administration} at 50 (2006)} To intercept these kinds of communications, filters (“packet-sniffers”)\footnote{A packet sniffer (a network diagnostic tool also known as a network analyzer) is computer software or hardware that can intercept and log traffic passing over a digital network or part of a network. As data travels over the monitored network segment, the sniffer can log each packet: an unfiltered sniffer captures all passing traffic and a filtered sniffer captures only those packets containing a specified data element. Captured packets must then be decoded, analyzed, and reassembled into a coherent message.\footnote{Because packets that are part of the same communication can travel different routes, or because their point of origin or destination can be masked using certain proxy routing techniques (for example, through networks like TOR that use “onion” routing), search strategies covering multiple nodes (or covering multiple entry and exit points on proxy networks) may be needed to effectively intercept any particular communication.\footnote{A familiar example of a packet sniffing application was the Federal Bureau of Investigation’s DCS-1000 application for lawful intercepts of email traffic (\textit{aka} “Carnivore”) (the FBI no longer uses DCS-1000, relying instead on commercial applications and the in house capabilities of Internet service providers for lawful intercepts). The DCS-1000 was intended to scan email traffic and only pick out and log material that was authorized under the particular search warrant pursuant to which it was being employed. See \textit{Carnivore Diagnostic Tool}, Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, before the U.S. Senate Committee on the Judiciary (Sep. 6, 2000). Although details of the DCS-1000 remain classified, it is believed that it consisted of a single-purpose Windows 2000/NT computer employing the DragonWare software suite, including: Carnivore, an analytic filter packet sniffer to capture packets; Packeteer, an application to reassemble packets into coherent messages, and Coolminer, an analytic tool to help analyze the intercepted data. The use of DCS-1000 in practice highlights the very problem discussed in this article—it is increasingly technically difficult—maybe impossible—to intercept only targeted communications in a packet-based communications network. For example, according to an internal FBI memo, technicians threw out legitimate wiretap information from an investigation of Osama bin Laden's terrorist network when the DCS...}} and search strategies\footnote{A familiar example of a packet sniffing application was the Federal Bureau of Investigation’s DCS-1000 application for lawful intercepts of email traffic (\textit{aka} “Carnivore”) (the FBI no longer uses DCS-1000, relying instead on commercial applications and the in house capabilities of Internet service providers for lawful intercepts). The DCS-1000 was intended to scan email traffic and only pick out and log material that was authorized under the particular search warrant pursuant to which it was being employed. See \textit{Carnivore Diagnostic Tool}, Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, before the U.S. Senate Committee on the Judiciary (Sep. 6, 2000). Although details of the DCS-1000 remain classified, it is believed that it consisted of a single-purpose Windows 2000/NT computer employing the DragonWare software suite, including: Carnivore, an analytic filter packet sniffer to capture packets; Packeteer, an application to reassemble packets into coherent messages, and Coolminer, an analytic tool to help analyze the intercepted data. The use of DCS-1000 in practice highlights the very problem discussed in this article—it is increasingly technically difficult—maybe impossible—to intercept only targeted communications in a packet-based communications network. For example, according to an internal FBI memo, technicians threw out legitimate wiretap information from an investigation of Osama bin Laden's terrorist network when the DCS...}} are deployed at various communication nodes (i.e., switches) to scan and filter all passing traffic with the hope of finding and extracting those packets of interest and reassembling them into a coherent message. Even targeting a specific message from a known sender may require scanning and filtering the entire communication flow at multiple nodes.\footnote{A familiar example of a packet sniffing application was the Federal Bureau of Investigation’s DCS-1000 application for lawful intercepts of email traffic (\textit{aka} “Carnivore”) (the FBI no longer uses DCS-1000, relying instead on commercial applications and the in house capabilities of Internet service providers for lawful intercepts). The DCS-1000 was intended to scan email traffic and only pick out and log material that was authorized under the particular search warrant pursuant to which it was being employed. See \textit{Carnivore Diagnostic Tool}, Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, before the U.S. Senate Committee on the Judiciary (Sep. 6, 2000). Although details of the DCS-1000 remain classified, it is believed that it consisted of a single-purpose Windows 2000/NT computer employing the DragonWare software suite, including: Carnivore, an analytic filter packet sniffer to capture packets; Packeteer, an application to reassemble packets into coherent messages, and Coolminer, an analytic tool to help analyze the intercepted data. The use of DCS-1000 in practice highlights the very problem discussed in this article—it is increasingly technically difficult—maybe impossible—to intercept only targeted communications in a packet-based communications network. For example, according to an internal FBI memo, technicians threw out legitimate wiretap information from an investigation of Osama bin Laden's terrorist network when the DCS...}}
Further, with the globalization of the telecommunications industry in recent years and the dominance of U.S. infrastructure providers, a large volume of international-to-international voice and email traffic is now routed through switches in the United States. A voice call from Europe to Asia, for example, may routinely go through a switch in the United States, and much of the world’s email traffic—even messages sent between regionally neighboring states, say Pakistan and Sudan—may now pass through switches in the United States. 40 In addition, a significant amount of web content and email is hosted on U.S.-based servers. The growth of this ‘transit traffic’ is problematic for foreign intelligence surveillance because if FISA were to be applied strictly according to its terms prior to any electronic surveillance of communication flows where the acquisition occurs in the U.S. or there is a substantial likelihood of intercepting “U.S. persons” communications (since domestic U.S. traffic transits the same switches), then no electronic surveillance of any kind could occur anywhere without a warrant and there is no procedure within FISA that would accommodate this need. 41

Modern network diagnostic tools, such as the Narus STA 6400 semantic traffic analyzer, give intelligence and law enforcement agencies powerful capabilities to monitor communications network activity. However, existing laws and procedures, including those in FISA, must be updated to accommodate technical and operational needs for their lawful employ while still protecting privacy and civil liberties.

40 It is rumored that it was a reluctance to disclose how much international traffic transited U.S. switches, among other things, that dissuaded the administration from asking Congress for amendments to FISA to address this particular problem and that then ultimately led to the secret authorization of the Terrorist Surveillance Program. Attorney General Alberto Gonzales has stated that the Bush administration chose not to ask Congress for an amendment to FISA to authorize such wiretaps explicitly because it would have been difficult to get such an amendment without compromising classified information relating to operational details. See Department of Homeland Security, White House Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005); and Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act (Dec. 21, 2005).

41 See generally, James Risen, supra note 36 at 42-60 (discussing the perceived need to circumvent FISA procedures); and see Eric Lichtblau & James Risen, supra note 33:

One issue of concern to the [FISC] … is whether the court has legal authority over calls outside the United States that happen to pass through American-based telephonic "switches" … "There was a lot of discussion about the switches" … the gateways through which much of the communications traffic flows. … The switches are some of the main arteries for moving voice and some Internet traffic into and out of the United States, and, with the globalization of the telecommunications industry in recent years, many international-to-international calls are also routed through such American switches. … The growth of that transit traffic had become a major issue for the intelligence community, officials say, because it had not been fully addressed by 1970's-era laws and regulations … . Now that foreign calls were being routed through switches on American soil, some judges and law enforcement officials regarded eavesdropping on those calls as a possible violation of those decades-old restrictions, including the [FISA], which requires court-approved warrants for domestic surveillance.

But see note 34 supra and note 44 infra discussing the FISC orders and the use of anticipatory warrants.
Collateral Intercepts: The globalization of communications.

Another problem—somewhat orthogonal to that presented by transit intercepts—also arises when FISA is triggered by foreign intelligence collection conducted against communications “to or from a person in the United States” or against “U.S. persons” in these globalized communication networks. Advances in information technology, the borderless nature of terrorist threats, and global communications that may travel on random paths across political borders has made place-of-collection and U.S. personhood an increasingly unworkable basis for controlling the collection of intelligence because it is in many cases no longer technically possible to determine exactly when a communication is taking place “to or from the United States” and no practical means exists to determine if a particular participant is a U.S. person or not until after further investigation. 42 “In fact, it is now difficult to tell where the domestic telephone system ends and the international network begins.” 43 FISA does not account for this.

Thus, where collateral U.S. person communications are intercepted incidental to a legitimate foreign intelligence intercept, there is no explicit way 44 consistent with FISA

---

42 Place-of-collection and citizenship of persons involved in the communication are increasingly arbitrary (in a technical sense) attributes of the intercepted communication, that is, these attributes are not obviously apparent or discernable from the place of interception or even from the communication itself. Publicly available intelligence guidelines discussing traditional operational assumptions—for example, that intercepts abroad are assumed to not target U.S. persons and those within the U.S. are—seem outdated as well. That place of collection and U.S. person rules are increasingly unworkable for information sharing is discussed in Markle Task Force on National Security in the Information Age Third Report, Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment at 32-41 (2006) (advocating replacing place of collection and U.S. persons rules with an “authorized use” standard for information sharing).

43 James Risen, supra note 36 at 50. Note also that one can now acquire and use from anywhere in the world a Voice over Internet Protocol (“VoIP”) telephone that has a local telephone number assigned in any area or country code desired. Some Jihadist websites specializing in countermeasure tradecraft have suggested acquiring VoIP telephones with domestic U.S. telephone numbers precisely so as to make surveillance more difficult by appearing to be domestic or U.S. person protected communications.

44 Communications of a U.S. person (or to or from the U.S.) acquired incidental to a lawful foreign collection are generally subject to minimization procedures consistent with Executive Order 12,333. While such information could be retained and disseminated according to intelligence guidelines if it amounted to foreign intelligence or counterintelligence, it could not in practice be the basis for developing probable cause for further targeting (that is, the basis for a FISA warrant application) if its foreign intelligence value was not apparent on its face (that is, if it required follow up investigation, additional surveillance, or sharing for context). Further, as discussed in notes 33 and 34 supra, if the collateral interception occurred while conducting foreign surveillance at a switch in the United States, the interception itself might trigger FISA requirements, thus, the information could not be used even if it evidenced probable cause on its face unless the original interception was somehow authorized. (And, there is no explicit FISA procedure for pre-authorizing such an interception, see the last paragraph of note 34 supra.)

According to official statements, the TSP mitigated part of this problem by explicitly authorizing collateral intercepts of international communications under Presidential authority where one party to the communication is a legitimate target of foreign intelligence surveillance (i.e., a suspected terrorist) even if the other party was in the U.S. or a U.S. person. Such surveillance is now subject to the FISC orders referred to in the Attorney General’s letter, supra note 2:
as currently constituted to engage in follow up electronic surveillance to determine if probable cause exists to target that individual, \(^{45}\) even though the collateral intercept itself may give rise to a Constitutionally reasonable suspicion. \(^{46}\)

*Automated analysis: content filtering, traffic analysis, and link or pattern analysis.* \(^{47}\)

Automated screening can monitor data flows to uncover terrorist connections or terrorist communication channels without human beings ever looking at anybody's emails or listening in on their phone calls. Only when the computer identifies suspicious connections or information do humans get involved. \(^{48}\)

---

I am writing to inform you that on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. It is unlikely that the new orders cover the entirety of the collateral intercept problem discussed in this article, but, in any case, FISA should be amended to provide an explicit statutory basis for these orders. The Justice Department has indicated that it is not prepared to make the FISC orders public, *see* Government’s Supplemental Submission, *supra* note 10 at 20 (“the longstanding practice is that FISA Court orders remain classified and not subject to public dissemination because, among other things, publication of FISA Court orders would notify the enemy of our targets and means of conducting surveillance”). Speculation about the nature of the FISC orders has included discussion of whether they include “anticipatory warrants” that would permit surveillance in the future if certain factual predicates occurred. Anticipatory warrants would allow a judge to agree ahead of time that if certain facts were to occur (for example, if a legitimate foreign target were to communicate to or from the U.S.), then probable cause would exist at that time for that communication and monitoring could take place under the warrant. The use of anticipatory warrants was upheld in *U.S. v. Grubbs*, 547 U.S. ___ (2006) (No. 04-1414 decided Mar. 21, 2006) (warrant containing “triggering conditions” is Constitutional). Although the use of anticipatory warrants to authorize collateral intercepts in these circumstances would meet the original intent of FISA, an explicit statutory basis should be enacted to support such orders.

\(^{45}\) Although FISA permits applications for warrants to be made up to 72 hours after the fact in certain limited emergency situations, 50 U.S.C. § 1805(f), these procedures do not address the collateral intercept problem discussed in this article or the TSP problem discussed in note 34 *supra* because they impose the same *a priori* requirements, that is, the Attorney General must determine *before* approving the surveillance that the “factual basis for issuance of an order under [FISA] to approve such surveillance exists,” even in cases where additional investigation or surveillance might be needed to determine such (or, in cases of incidental communications to or from the U.S., where the communication itself could not be anticipated).


\(^{47}\) Parts of this subsection are adapted from Taipale, *Whispering Wires*, *supra* note 35.

It is beyond the scope of this article to explore all the different analysis techniques that can be applied to the automated monitoring of terrorist communications but three generic examples show the range of activity possible: content filtering, traffic analysis, and pattern or link analysis.

Content filtering is used to search for the occurrence of particular words or language combinations that may be indicative of particular communications (or persons) of interest. A simple example of this would be to screen for messages to or from known terrorist sources containing the words “nuclear weapon” or “osama bin laden”. Actual search algorithms are, of course, much more complex and sophisticated and can employ artificial intelligence, machine learning, and powerful statistical methods such as Bayesian analysis to identify “signals of interest.” It should be made clear that the filtering contemplated here is not the same as undirected “data mining” in which all communication flows are screened looking for previously unknown general indicia of suspicion with no starting point.

Traffic analysis is the observation of traffic patterns—message lengths, frequency, paths, etc.—of communications without examining the content of the message (traffic analysis can be used even where content is encrypted). Traffic analysis can reveal patterns of organization, for example, by measuring “betweenness” in email traffic or other communications among known or suspected terrorists or terrorist communication channels or networks. By looking for patterns in traffic these techniques, together with analytical methods such as social network theory, can identify organizations or groups and the key people in them. These methods can uncover how terrorist groups are

49 For example, the Echelon program is thought to be an NSA program (in partnership with corresponding agencies in Canada, the U.K., Australia and New Zealand) to automatically filter and sort intercepted foreign communications using “dictionaries” consisting of targeted keywords—names, addresses, telephone numbers, IP addresses, aliases, affiliates, etc.—for different categories of targets. Patrick Radden Keefe, CHATTER at 116 (2006). The existence of Echelon has not been officially acknowledged and the details of the program are classified. However, most public accounts describe a process in which communications are flagged by certain keywords. See, e.g., Federation of American Scientists web site at http://www.fas.org/irp/program/process/echelon.htm; European Parliament, Temporary Committee on the ECHELON Interception System, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098-INI) (Jul. 11, 2001). And, see U.S. Patent 6,169,969 for a “device and method for full-text large dictionary string matching” discussed in Keefe, supra at 121-122.

50 See discussion of link and pattern analysis below.

51 See Bruce Schneier, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD at 34-35 (2000) (“Traffic analysis is the study of communication patterns … [o]ften the patterns of communication are just as important as the contents of communications”).

52 Links with high “betweenness” are those infrequently used links that connect groups from two distinct communities of frequently connected individuals. See generally Linton C. Freeman. A set of measures of centrality based on betweenness, SOCIOMETRY, Vol. 40 No. 1, 35–41 (Mar. 1977).

53 Covert social networks exhibit certain characteristics that can be identified. Post-hoc analysis of the 9/11 terror network shows that these relational networks exist and can be identified, at least after the fact. Vladis E. Krebs, Uncloaking Terrorist Networks, FIRST MONDAY (mapping and analyzing the relational network among the 9/11 hijackers). Research on mafia and drug smuggling networks show characteristics particular to each kind of organization, and current social network research in
organized and reveal activity even if they are communicating in code or only discussing the weather. 54

Link or pattern analysis in this context is the use of observed or hypothesized connections or patterns to find other related but unknown relationships. Again, it is important to distinguish undirected “data mining” for general patterns of suspicion from the targeted use of pattern matching to allocate investigative resources being discussed here. 55

For example, known patterns of terrorist communications can be identified and used to uncover other unknown but indirectly related terrorists. Thus, for instance, in the immediate aftermath of 9/11 the FBI determined that the leaders of the 19 hijackers had made 206 international telephone calls to locations in Saudi Arabia, Syria, and Germany. 56 It is believed that in order to determine whether any other unknown persons—so-called sleeper cells—in the United States might have been in communication with the same pattern of foreign phone numbers the NSA analyzed Call Data Records (CDRs) of international and domestic phone calls obtained from the major telecommunication


54 See, e.g., Hazel Muir, Email Traffic Patterns can Reveal Ringleaders, NEW SCIENTIST (Mar. 27, 2003). For a general discussion of the use of social network theory in counterterrorism analysis, see Patrick Radden Keefe, Can Network Theory Thwart Terrorists? N.Y. TIMES (Mar. 12, 2006).

55 It is beyond the scope of this article to discuss general data mining issues in greater detail. For a detailed discussion of these and related issues, see K. A. Taipale, Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data, 5 COLUM. SCI. & TECH. L. REV. 2 (2003) (hereinafter, Connecting the Dots). For a detailed rebuttal of popular arguments against the potential usefulness of data mining for counterterrorism applications, see The Privacy Implications of Government Data Mining Programs, Testimony of Kim Taipale before the U.S. Senate Committee on the Judiciary at 6-16 (Jan. 10, 2007) (“popular arguments about why [data mining] won’t work for counterterrorism are simply wrong—… the commercial analogy is irrelevant, the ‘training set’ problem is a red herring, and the false positive problem can be significantly reduced by using appropriate architectures—and, in any case, is not unique to data mining.”) See Transcript of Oral Testimony, id.)

56 John Crewdson, Germany says 9/11 hijackers called Syria, Saudi Arabia, CHI. TRIB. (Mar. 8, 2006) (“According to [a classified report based on telephone records obtained from the FBI], 206 international telephone calls were known to have been made by the leaders of the hijacking plot after they arrived in the United States—including 29 to Germany, 32 to Saudi Arabia and 66 to Syria.”)

57 That is, to uncover others who may not have a direct connection to the 19 known hijackers but who may exhibit the same or similar patterns of communication as the known hijackers.
companies.\textsuperscript{58} Undertaking such an analysis seems reasonable, particularly in the circumstances immediately following 9/11, yet, FISA and existing procedures do not provided an authorizing mechanism for determining such reasonableness because FISA simply did not contemplate the need for approval of specific—but not individualized—pattern-based data searches or surveillance.\textsuperscript{59}

It is important to point out again that the kind of automated analysis being discussed in this section is not the undirected “data mining” to look for general indicia of “suspicious behavior” that rightly has libertarians\textsuperscript{60} and civil libertarians\textsuperscript{61} alike concerned about fishing expeditions or general searches to examine all communication flows in the manner of a general warrant.\textsuperscript{62} These automated monitoring technologies should not be employed as a general method for “finding terrorists” by screening all global communications with no starting point, nor should they be used for determining guilt or

\textsuperscript{58} That the NSA obtained CDRs from U.S. telecommunication carriers for analysis was implied in Lichtblau, \textit{supra} note 41, and was explicitly alleged in Cauley, \textit{supra} note 2.

\textsuperscript{59} FISA specifically includes procedures for use of so-called pen register or trap and trace devices to record addressing details from phone conversations under a lower standard than that required for content interception (i.e., lower than that required for “wiretaps”), §1842, however, it provides no mechanism for authorizing searches for specific traffic information from general databases.

It is commonly settled law under Smith v. Maryland, 442 U.S. 735 (1979), that addressing information is generally entitled to lesser Constitutional protection than communication content. \textit{See generally} \textit{CONGRESSIONAL RESEARCH SERVICE, GOVERNMENT ACCESS TO PHONE CALLING ACTIVITY AND RELATED RECORDS: LEGAL AUTHOIRITIES}, CRS RL33424 (May 17, 2006). Further, the particularity requirement of the Fourth Amendment does not impose an irreducible requirement of individualized suspicion before a search can be found reasonable, or even to procure a warrant. In at least six cases, the Supreme Court has upheld the use of drug courier profiles as the basis to stop and subject individuals to further investigative actions, including search. More relevant, the court in United States v. Lopez, 328 F. Supp 1077 (E.D.N.Y. 1971), upheld the validity of hijacker behavior profiling, opining that “in effect ... [the profiling] system itself ... acts as informer” serving as sufficient Constitutional basis for initiating further investigative actions. Yet, FISA simply provides no mechanism to address the need for authorization in the described circumstances.

\textsuperscript{60} \textit{See, e.g.}, Testimony concerning the Privacy Implications of Government Data Mining Programs by Robert Barr, Chief Executive Officer, Liberty Strategies, LLC; and Testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute to the Senate Judiciary Committee Hearing Entitled “Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs” before the U.S. Senate Committee of the Judiciary (Jan. 10, 2007).

\textsuperscript{61} \textit{See, e.g.}, Statement of Leslie Harris, Executive Director, Center for Democracy & Technology, Before the U.S. Senate Committee on the Judiciary “Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs” (Jan. 10, 2007); and see Jay Stanley & Barry Steinhardt, \textit{Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society} at 11-12, ACLU (Jan. 2003).

\textsuperscript{62} \textit{See, e.g.}, Taipale, \textit{HPSCI Testimony, supra} note 46 at 5-6 (“Programs of surveillance are not general warrants”). It is the use of general warrants by the English that led in part to the American Revolution, \textit{see, e.g.}, O.M. Dickerson, \textit{Writs of Assistance as a Cause of the Revolution}, in \textit{THE ERA OF THE AMERICAN REVOLUTION} (Richard Morris ed. 1939), and to enactment of the Fourth Amendment, \textit{see Edward Corwin, THE CONSTITUTION AND WHAT IT MEANS TODAY} at 341 (1978, 1920); David Hutchinson, \textit{THE FOUNDATIONS OF THE CONSTITUTION} (1975, 1928).
innocence. Rather, they should be employed carefully—subject to appropriate authorizations and effective oversight—as powerful tools to help better allocate law enforcement and security resources to more likely targets. As such, automated analysis is simply the computational automation of traditional investigative procedures—monitoring known or suspected terrorists, following links from these suspects, or looking for specific patterns of operations or behaviors (i.e., observing and anticipating *modus operandi*).

FISA as currently constituted is simply unworkable in the context of globalized communications networks and advanced technical methods for gathering intelligence because it provides no mechanisms to adequately address the authorization and oversight of transit intercepts, collateral intercepts, and the use of automated monitoring. To simply insist that these problems be ignored or that the solution lies only in streamlining cumbersome procedures is to engage in policy-making in a dangerous state of denial reminiscent of King Ludd. Nor is it adequate as a matter of public policy for “innovative” interpretations of existing FISA requirements enacted through secret FISC orders to resolve the debate. What is needed, in my view, is a rethinking of foreign

---


64 One of the criticisms of using predictive risk management techniques for counterterrorism is that these methods may cast a wide net of “suspicion” and that many of these “suspects” will be innocent. *See, e.g.*, Stanley & Steinhardt, supra note 61; Jeff Jonas & Jim Harper, *Effective Counterterrorism and the Limited Role of Predictive Data Mining*, Cato Institute (December 11, 2006). Yet, such an assumption is not uncritically warranted as these critics confuse the use of probability-based resource allocation for investigative purposes with the assignment or determination of guilt (nee “suspicion”).

For example, if police departments use CompStat or other statistical analysis to assign resources—say more beat officers—to a high crime neighborhood, we do not make the inference that everybody in that neighborhood is a suspect, only that assigning resources there may be more effective than elsewhere. So, too, in counterterrorism, computational analytic tools can help allocate intelligence and law enforcement resources more effectively so long as care is taken to design policy and systems to avoid automatically triggering adverse consequences—such as determining guilt or innocence—without adequate opportunities for error correction and redress. *See also K. A. Taipale, The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence*, IEEE INTELLIGENT SYSTEMS, Vol. 20 No. 5, 80–83 (Sept./Oct. 2005) (“… it is the probative value of the evidence, rather than its probabilistic nature, that is relevant in determining whether it is a sufficient predicate for government action. To argue otherwise is to confuse the presumption of innocence with the probability of innocence.” *Id.* at 82).

65 For example, as proposed in the Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act (“LISTEN Act”) (HR5371).

66 *See Taipale, Frankenstein*, at 126-127, 220-221 (arguing that the lesson to be drawn from the experience of the *luddites* is that simple opposition to technological change is doomed to failure and therefore adaptation is a better policy).

67 The Attorney General has described the FISC orders as “innovative” and “complex” requiring two years of negotiations between the administration and the FISC:

> These orders are innovative, they are complex and it took considerable time and work for the Government to develop the approach that was proposed to the Court and for the Judge on the FISC to consider and approve these orders.

Letter of the Attorney General, *supra* note 2. And, in a background briefing by two “senior Justice Department officials”:...
intelligence surveillance that takes into account the changed security and technology context, and a careful updating and amending of FISA and related procedures to specifically meet these challenges—including, if appropriate, an explicit statutory basis for the existing FISC orders—while still upholding core Constitutional principles. 68

Section III: Fixing Foreign Intelligence Surveillance.

To address the deficiencies identified in the previous section, FISA should be amended to provide for:

1. explicit authority or programmatic pre-approval 69 without requiring individual warrants for transit intercepts, that is, intercepts “at the switch” aimed at foreign

These orders, however, are orders that have taken a long time to put together, to work on. They're orders that take advantage of use of the use of the FISA statute and developments in the law. I can't really get into developments in the law before the FISA court. But it's a process that began nearly two years ago, and it's just now that the court has approved these orders.


But, “[t]he legality of this … surveillance program should not be decided by a secret court in one-sided proceedings.” Press Release, ACLU Demands More Information on "Innovative" Orders Issued by Secret Court, American Civil Liberties Union (Jan. 17, 2007). For speculation about the nature of the FISC orders, see notes 34 and 44 supra.

68 Even following the issuance of the FISC orders, the administration also still believes that FISA needs updating:

[W]e in the administration continue to believe that Congress should enact FISA reform legislation to modernize FISA statute to reestablish what we think is the proper, original focus of FISA on the domestic communications of U.S. persons. We believe that debate should continue to happen, that Congress should consider modernizing FISA very quickly in the new Congress.

Transcript, supra note 67.

69 It is beyond the scope of this article to recommend particular mechanisms or standards for authorizing such programmatic approvals. It has been argued that courts are ill-suited, and may be constitutionally prohibited, from such an oversight role, see, e.g., David B. Rivkin, Jr. and Lee A. Casey, Commentary: Inherent Authority, WALL ST. J. A16 (Feb. 8, 2006) (“The federal courts can only adjudicate actual cases and controversies; they cannot offer advisory opinions”), and that a statutory executive or legislative authorization or oversight body should be created. Compare, for example, the proposed Terrorist Surveillance Act of 2006 (the DeWine bill) that would approve the Terrorist Surveillance Program subject to oversight by special Congressional committees with the proposed National Security Surveillance Act of 2006 (the Specter bill) that would require FISA court (FISC) approval and oversight, including review every 45 days to continue "electronic surveillance programs." See also, Taipale, HPSCI Testimony, supra note 46 at 10-12 (discussing the pros-and-cons of judicial versus legislative involvement) and see John Schmidt, Together Against Terror, LEGALTIMES (Jan. 15, 2007) (arguing persuasively for a legal structure that involves the courts in order to foster the necessary confidence in the legality of the surveillance activity). Cf. also H.R. 5825 (109th Congress) Electronic Surveillance Modernization Act (the Wilson bill) (passed by the House on Sep. 28 and referred to the Senate Committee on the Judiciary), which would require Congressional oversight but allow submission of the TSP to the FISC for review.

Although it is unclear exactly the scope of the current FISC orders, the administration has denied that they are “programmatic” in the advisory sense:
communications but that might currently trigger statutory FISA warrant requirements
because the acquisition “occurs in the U.S.” (or elsewhere with the “likelihood that
the surveillance will [also] acquire the contents of any communication to which a
United States person is a party”),

2. programmatic pre-approval \(^{71}\) without requiring individual warrants of \textit{automated analysis} and monitoring methods, including targeted content filtering, traffic analysis, and link or pattern analysis in specific contexts where the initial target or channel is a legitimate foreign intelligence target but the surveillance takes place within the U.S. or there is a likelihood of intercepting U.S. persons, \(^{72}\) and

3. the statutory equivalent of a \textit{Terry stop} \(^{73}\) to permit limited follow up electronic surveillance of suspicious communications, including those involving U.S. persons, \textit{collaterally intercepted} incidental to an authorized surveillance (including incidental to those authorized through programmatic approval under (1) and (2) above).

It is beyond the scope of this article to examine the related Constitutional jurisprudence in detail. \(^{74}\) However, there is likely no Constitutional prohibition to a carefully crafted legislative solution that would statutorily authorize programmatic approval of electronic surveillance programs for foreign intelligence purposes that (i) target foreign communications transiting the U.S. or (ii) use automated analysis or monitoring methods, and which would also authorize limited follow-up investigation or surveillance based on reasonable suspicion of U.S. persons initially identified through collateral intercepts in order to determine if probable cause sufficient to meet FISA requirements for a warrant could be established. \(^{75}\)

---

70 Note that these are statutory warrant requirements, not Constitutionally requirements. \textit{See} Taipale, \textit{HPSCI Testimony}, supra note 46 at 8-9 (discussing Constitutional warrant requirements).

71 See note 69.

72 Note that under some intelligence collection guidelines, electronic data is generally not considered “collected” until it has been processed into intelligible form. \textit{See}, e.g., Department of Defense Directive 5240.1-R \textit{Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons} at 15 §C2.2.1 (1982). Thus, bringing automated analysis under a statutory scheme might actually provide more oversight for some activity than under current guideline.

73 \textit{Terry v. Ohio}, 392 U.S. 1 (1968) (holding that a police officer may stop an individual on the basis of “reasonable suspicion” and conduct a limited follow up search prior to establishing probable cause).


75 Note also that Attorney General Gonzales has stated that: “the standard applied [in the NSA Terrorist Surveillance Program]—‘reasonable basis to believe’—is essentially the same as the traditional
Further, permitting such programs may actually be preferable—and, ultimately, less intrusive to civil liberties—than alternative methods, for example, requiring physical surveillance to independently establish probable cause following a determination of reasonable suspicion incidental to a legitimate foreign intelligence intercept.

What is needed is an explicit statutory mechanism, incorporating the necessary democratic checks-and-balances, for programmatic approval of transit intercepts and automated analysis targeted against known or reasonably suspected foreign terrorist communication sources—that is, against legitimate foreign intelligence targets normally not subject to FISA and normally not requiring a warrant—even where such surveillance or technical methods may “occur in the United States” or where there is a likelihood of intercepting U.S. persons communications. If the initial process identifies potentially suspicious connections to or from legitimate foreign intelligence targets—including, for example, U.S. persons or sources communicating with known or suspected terrorists or through known or suspected terrorist communication channels—then some additional appropriately authorized monitoring or follow-up investigation (including technical analysis, monitoring, or additional circumscribed electronic surveillance) should be permitted in order to determine if that initial “reasonable suspicion” is justified.

Fourth Amendment probable cause standard.” Prepared Remarks for Attorney General Alberto R. Gonzales at the Georgetown University Law Center (Jan. 24, 2006). And, further, that the current FISC orders are based on “probable cause.” See Gonzales letter, supra note 2 and Transcript, supra note 67. For an overview of Fourth Amendment probable cause and reasonable suspicion standards, see Congressional Research Service Memorandum to the Senate Select Committee on Intelligence, Probable Cause, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act (Jan. 30, 2006) (“… the [Supreme] Court has pointed out that probable cause is the description of a degree of probability that cannot be easily defined out of context.” Id. at CRS-2.)

Thus, there are two related issues involved here: first, whether there are actually two standards—reasonable suspicion and probable cause; and, second, who—a FISC judge following lengthy a priori FISA procedures or a “shift-supervisor” [senior intelligence officer] at the NSA in “hot pursuit” of an intercepted communication—makes the determination. A Terry-like procedure would address both by leaving some discretion with the “officer on the scene” (see, Terry) but subject to explicit statutory procedures and a Constitutional standard of reasonableness.

76 Incidental intercepts of U.S. person data is currently subject to minimization procedures that prevent effective use of such collateral information unless it has foreign intelligence or counterintelligence (or in some cases, criminal intelligence) value on its face. Further use or dissemination of such information is restricted—for example, by blocking out the name or phone number of U.S. persons—in a way that does not, in practice, permit it to be used to develop independent probable cause to target that U.S. person. (Prior to 9/11 such information was not even shared with other government agencies except upon their request.) And, as discussed above in notes 34 and 44 supra, in cases where incidental intercepts trigger FISA only because they “occur in the United States” such information cannot subsequently be used unless the original interception is specifically authorized. Indeed, it appears that concern over the use of information from the TSP intercepts to establish probable cause for subsequent FISA warrant applications may have led to a three week suspension of the TSP in 2004. See Carol D. Leonnig, Secret Court's Judges Were Warned About NSA Spy Data, WASH. POST (Feb. 9, 2006). This then suggests another way to deal with this particular aspect of the collateral intercept problem by changing the minimization procedures to explicitly permit some limited follow-up investigation or surveillance (as suggested above under the Terry stop equivalent) and to sanction the use of information gleaned during this period (or otherwise collateral to a programmatic intercept) for subsequent warrant applications.
The problem with FISA is that it contemplates only a single binary \textit{a priori} threshold for authorizing any electronic interception within the U.S. or involving U.S. persons — probable cause that the target is an agent of a foreign power. \footnote{Assuming that the current FISC orders conform to the speculation regarding “anticipatory warrants,” \textit{see note 44 supra}, then what the administration and the FISC seem to have done is essentially pre-negotiate the future factual circumstances that would be probable cause if they were to occur—that is, to anticipate foreign target communications to or from a person in the United States and anticipatorily sanction those for interception should they occur. Such a process would have greater legitimacy—that is, a greater claim to be recognized as right and just, \textit{see generally} Jurgen Habermas, \textit{COMMUNICATION AND THE EVOLUTION OF SOCIETY} at 178 (1976) (discussing “legitimacy”)—if it were subject to explicit statutory authority and procedures. \textit{See also} Schmidt, \textit{supra} note 69 (arguing for legislation to explicitly extend the FISC jurisdiction to allow programmatic approval).} Unfortunately, even extensive contact with a known terrorist may not be procedurally sufficient to meet the current requirements of FISA yet may have significant “foreign intelligence value” requiring follow up investigation (and would also meet the Constitutional requirement of reasonableness).

Thus, what is needed in my view, is the electronic surveillance equivalent of a \textit{Terry} stop, the Constitutionally permissible procedure under which a police officer can briefly detain someone for questioning and conduct a limited pat-down search if they have "reasonable suspicion" to believe that the person may be involved in a crime. \footnote{See Taipale, \textit{Whispering Wires}, \textit{supra} note 35 (discussing the “electronic surveillance equivalent of a \textit{Terry} stop”).} In the case of electronic surveillance, this would permit a circumscribed but authorized procedure for follow-up monitoring or investigation of initial suspicion derived from automated monitoring (or otherwise developed collateral to a legitimate foreign intelligence intercept).

If ongoing suspicion is not justified on follow-up analysis or surveillance, monitoring would be discontinued and normal (or enhanced \footnote{Normal minimization procedures are intended to limit retention or use of incidentally acquired U.S. person information without foreign intelligence value. A statutory regime that allowed collateral intercepts and sanctioned the use of collaterally collected information subject to programmatic approvals to establish independent predicate for additional warrants might require enhanced minimization procedures to isolate analysis of collateral information. As discussed in note 76 \textit{supra}, it appears that the FISC orders include enhanced minimization procedures.}) minimization procedures would be
triggered, however, if suspicion is reasonably justified then monitoring could continue under the programmatic approval for some limited further period to determine if standard statutory probable cause can be established. If there is probable cause to suspect that the target is actively engaged in terrorism or is an “agent” of a foreign terrorist group, then a regular FISA warrant would be sought to target that U.S. person or source for full surveillance.

Based on published reports and public statements by intelligence officials responsible for the Terrorist Surveillance Program it is my belief that this indeed describes generally the procedures that the TSP was following, and that are currently being authorized under the FISC orders.

Conclusion.

What is needed then is to provide a statutory mechanism that involves Congressional authorization and oversight, together with an explicit statutory basis for judicial orders and review, so that legitimate foreign intelligence requirements can be met without resorting to unilateral secret executive branch approvals or by shoehorning “innovative” solutions not explicitly anticipated under FISA. Regardless of whether the President indeed currently has statutory or inherent authority to approve such programs, or whether a FISC judge can be convinced to “stretch” FISA to cover certain needs, our system of government works best, and public confidence is best maintained, only when the three branches of government work together in consensus and the broad parameters of procedural protections are publicly debated and agreed. Further, the ability of our government to respond appropriately to emergent national security threats is too important to be wholly dependant on the negotiation of ad hoc procedures during times of crises.

The issue with foreign intelligence surveillance in modern communication systems is under what conditions information derived from collateral intercepts from legitimate surveillance of foreign intelligence targets or through automated monitoring can itself provide the reasonable predicate to allocate additional investigative resources for follow up investigation or surveillance even when it involves “U.S. persons” or the when the communication takes place within the U.S. FISA currently provides no workable mechanism for addressing these circumstances and should be amended.


81 See generally notes 2, 34, 44, 67, 69, 75, 76, and 77 supra.

82 See note 2 and 67 supra.