THE EAR OF DIONYSUS: RETHINKING FOREIGN INTELLIGENCE SURVEILLANCE

K. A. TAIPALE*

9 YALE J. L. & TECH. 128 (2007)

TABLE OF CONTENTS

A précis of this article was published as *Rethinking Foreign Intelligence Surveillance*, WORLD POLICY J. (Vol. XIII No. 4, Winter 2006-2007), *available at* http://www.mitpressjournals.org/doi/pdf/10.1162/wopj.2007.23.4.77.

* *Kim Taipale is the founder and executive director of the Center for Advanced Studies in Science and Technology Policy. He is also a senior fellow at the World Policy Institute, a member of the Markle Task Force on National Security in the Information Age, and an adjunct professor of law at New York Law School. His other writings can be found online at http://taipale.info/.*

INTRODUCTION

As the 110th Congress begins to flex its atrophied oversight muscle,[1] it bears remembering that, in the ongoing debate over *who* should have the authority to authorize and oversee foreign intelligence surveillance programs,[2] *someone* must,[3] and the existing mechanisms, in particular, the Foreign Intelligence Surveillance Act of 1978 ("FISA")[4] and its related

---

[1] *See, e.g.*, Donna Leinwand, *Senators Press Gonzales on Delay in Getting Court Okay on Surveillance*, USA TODAY, Jan 19, 2007, at 4A; Lara Jakes Jordan, *Senators Grill Gonzales Over Spy Program*, SUN-SENTINEL (Fort Lauderdale, Fla.), Jan. 19, 2007, at 6A; Tom Brune, *Surveillance Questioned: Gonzales, Senate Judiciary Committee Battle Over Decision by Special Courts*, NEWSDAY, Jan. 18, 2007, at A26; *and* 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, 2006, *available at* http://www.iht.com/articles/2006/01/01/news/policy.php; 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 . . . ."); *and* Eric Lichtblau, *With Power Set to Be Split, Wiretaps Re-emerge as Issue,* N.Y. TIMES, Nov. 10, 2006, at A28 ("Democrats . . . vowed to investigate the [National Security Agency Terrorist Surveillance Program] aggressively once they assume power").

[2] 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"), s*ee* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1**,** 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), at A1. 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 on January 10, 2007 authorizing certain surveillance previously authorized under the NSA TSP (the "FISC orders"). 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. Letter from Alberto Gonzales, Attorney General of the United States, to Patrick Leahy, Chairman, and Arlen Specter, Ranking Member, Committee on the Judiciary, United States Senate (Jan. 17, 2007), *available at* http://fas.org/irp///agency/doj/fisa/ag011707.pdf.

[3] *See* Knowlton, *supra* note 1 ("[Senator] Schumer [D-NY] 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.").

[4] Pub. L. No. 95-511, Title I, 92 STAT. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, & 1861-62). FISA provides a framework for using electronic surveillance, physical searches, pen registers and trap and trace devices to acquire "foreign intelligence information."

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.

New technologies do not determine human fates, but they do alter the spectrum of potentialities within which people act.[5] 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.[6] 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[7] — rather, it argues that familiar, existing oversight and control mechanisms—including FISA—or their analogues can be applied in these novel, technologically-enabled circumstances, but only if the challenges and opportunities are better understood and the laws and procedures updated to accommodate needed change.

This article is intended neither as critique nor endorsement of any particular government surveillance program or action;[8] rather, it attempts to

[5] ROBERT MCCLINTOCK & K. A. TAIPALE, INSTITUTE FOR LEARNING TECHNOLOGIES AT COLUMBIA UNIVERSITY, EDUCATING AMERICA FOR THE 21ST CENTURY 2 (1994).

[6] 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 (Alan Sheridan trans., 1977). 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).

[7] 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 1009-12 (David Kamien ed., 2006); *and* 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, 126-8 (2004) (hereinafter, "*Frankenstein"*).

[8] In particular, neither of the classified programs referred to in note 2, *supra*; however, certain aspects of the TSP are discussed in general terms in Section III, *infra*.

highlight certain issues critical to a reasoned debate and democratic resolution of these issues. Further, this article does not address directly whether the President currently has inherent or statutory authority to approve any specific operational program[9] nor whether press disclosure of classified government programs is appropriate or justified.[10]

---

[9] Whether the President has inherent or statutory authority to authorize foreign intelligence surveillance programs, including the TSP, is currently being litigated. *See* ACLU v. NSA, No. 06-CV-10204 (E.D. Mich., filed Jan. 17, 2006); and 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"); *and* Editorial, *A Judicial Misfire*, WASH. POST, Aug. 18, 2006, at A20 (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. 26, 2007, at A5 ("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, at A12.

Testifying in 1976 that the President must retain 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"), President Gerald Ford's Attorney General Edward Levi asserted that there is "a presidential [surveillance] power which cannot be limited, no matter what Congress says." Levi, a well-respected constitutional scholar and formerly the dean of the University of Chicago Law School, testified that "[t]he very nature of the reserved presidential power, the reason it is so important, is that some kind of emergency could arise which I cannot foresee now, nor, with due deference to Congress, do I believe Congress can foresee." *Foreign Intelligence Surveillance Act of 1976, Hearing on S. 743, S. 1888 and S. 3197, before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary United States Senate*, 94th Cong., 17-18 (1976) (testimony of Edward H. Levi, Attorney General) quoted in John Schmidt, *When Terrorists Talk… ,* LEGALTIMES, Sep. 18, 2006 (discussing the exclusivity provision of FISA and the President's inherent surveillance power). In particular, 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 …

This article is organized into six parts: this *Introduction*, four descriptive sections, and a brief *Conclusion*. *Section I: Foreign Intelligence Surveillance: A Brief Overview* provides a very brief introduction to the relevant parts of the FISA regime; *Section II: 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 III: The Ear of Dionysus* 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 (this section also briefly speculates on certain aspects of the TSP); and, *Section IV: Fixing Foreign Intelligence Surveillance* suggests some potential solutions that preserve existing Fourth Amendment principles and protections while still addressing these failures. Finally, the *Conclusion*

---

not acknowledge the president's retained surveillance power" *Id.* (emphasis added). While I take no position in this article on whether, indeed, the President retains inherent surveillance powers, I do believe that the issues discussed herein are among those kinds of unforeseen circumstances that Levi foreshadowed.

[10] For example, on June 23, 2006, *The New York 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 institutions." Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror,* N.Y. TIMES, Jun. 23, 2006, at A1. Subsequently, *The New York 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, at A12. However, according to then House Intelligence Committee Chairman Pete Hoekstra (R-MI), "The mea culpa of the *New York 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, at A16 ("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 consideration of whether *The New York Times* violated the Espionage Act, 18 U.S.C. § 798 (2000) (Disclosure of classified information), when it disclosed the TSP, *see* Gabriel Schoenfeld, *Has the "New York Times" Violated the Espionage Act?* COMMENTARY, March 2006, at 23 ("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). *See also Digital Age with James C. Goodale: "Will Bush Indict The New York Times?"* (WNYE-PBS television broadcast, Mar. 4, 2007).

reiterates the need to get beyond backward looking recriminations and to craft progressive consensual solutions.

I. FOREIGN INTELLIGENCE SURVEILLANCE: A BRIEF OVERVIEW

Of relevance to the discussion in this Article,[11] FISA generally prescribes procedures requiring a court order for conducting electronic surveillance to gather "foreign intelligence information"[12] when such surveillance targets United States persons[13] or is conducted within the United States.[14] FISA was never intended to apply to wholly foreign communications of non-U.S. persons nor to be triggered by incidental interceptions of U.S. person communications during legitimate foreign intelligence intercepts not themselves subject to FISA.[15] However, as

[11] This article concerns itself with certain specific aspects of electronic surveillance—in particular the interception of 'signals of interest' in packet-based communication networks—and the related technology and policy developments. Thus, it is beyond the scope of this article to fully delineate FISA and the related foreign intelligence surveillance law. For a detailed discussion of FISA, *see* ELIZABETH B. BAZEN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND RECENT JUDICIAL DECISIONS, (Congressional Research Service Report for Congress No. RL30465, 2007).

[12] "Foreign intelligence information" is information that "relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power or (B) international terrorism by a foreign power or an agent of a foreign power . . . ." 50 U.S.C. § 1801(e) (2000).

[13] "United States person" means a U.S. citizen or lawfully resident alien. 50 U.S.C. § 1801(i) (2000).

[14] "Electronic surveillance" means—

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device 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, … ;
>
> …

50 U.S.C. § 1801(f) (2000)

[15] Communications of a U.S. person acquired during or incidental to a lawful foreign collection would generally be subject to minimization procedures consistent with Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted as amended in* 50 U.S.C. § 401 note, and related guideline documents. Part 2.3 (c) of the executive order would permit retention and dissemination of "information obtained in the course of a lawful … international terrorism investigation" subject only to normal minimization requirements. *See* note 54 *infra* and accompanying text. *Cf.* note 91 *infra* (discussing restrictions in practice that prevent

discussed in Section III below, technical developments unanticipated by FISA are triggering warrant requirements in circumstances that were not contemplated or intended when FISA was enacted.[16]

Further, FISA is intended to provide a statutory mechanism to authorize electronic surveillance of U.S. persons or within the U.S. when there is probable cause to believe the target is an "agent of a foreign

---

effective use in certain circumstances of incidental intercepts of U.S. person communications). Executive Order 12,333 allows the collection, retention, or dissemination of information about U.S. persons pursuant to procedures established by the head of each intelligence agency and approved by the Attorney General.

> The [Central Intelligence Agency] procedures are embodied in Headquarters Regulation (H.R.) 7-1 entitled, "Law and Policy Governing the Conduct of Intelligence Activities." NSA is governed by Department of Defense Directive 5240.1-R, "DoD Activities that May Affect U.S. Persons," including a classified appendix particularized for NSA [*see* partially declassified *Annex – Classified Annex to DoD Procedures under Executive Order 12,333* to NSA/CSS POLICY 1-23 (Mar. 11, 2004)]. The guidelines are further enunciated within NSA through an internal directive, [NSA/Central Security Services] U.S. Signals Intelligence Directive 18 [Jul. 27, 1993, hereinafter "USSID 18"]. The FBI procedures are contained in "Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations" [Mar. 1999] [these guidelines were updated and revised in *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (effective Oct. 31, 2003)].

NATIONAL SECURITY AGENCY, REPORT TO CONGRESS: LEGAL STANDARDS FOR THE INTELLIGENCE COMMUNITY IN CONDUCTING ELECTRONIC SURVEILLANCE (2000), *available at* http://www.fas.org/irp/nsa/standards.html.

[16] For example, when wholly foreign communications are targeted from a telecommunications switch in the United States and a communication "to or from the U.S." is incidentally intercepted, thus, implicating 50 U.S.C. § 1801(f)(2), see the discussion of transit and collateral intercepts in Section III, *infra*. *And see* notes 41 and 49 *infra*. Note that any implied warrant requirement in these circumstances is only a statutory requirement as there is no general Fourth Amendment requirement for a warrant for incidental collection from a lawful intercept. Even under the stricter provisions governing ordinary criminal electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), *codified at* 18 U.S.C. §§ 2510-2521, incidental interception of a non-targeted person's conversations during an otherwise lawful surveillance would not be a violation of the Fourth Amendment. *See* United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985); *and* United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973). Indeed, absent the FISA statute, there may be no general Fourth Amendment warrant requirement for any foreign intelligence surveillance. *See, e.g.,* United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980) (acknowledging the foreign intelligence exception to the Fourth Amendment warrant requirement); *see also* United States v. United States District Court [Keith], 407 U.S. 297, 321-22 (1972) (warrant required for domestic security electronic surveillance, but Court explicitly disclaims any intent to decide whether warrant clause applies to surveillance of foreign powers or their agents).

power,"[17] 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 "a group engaged in international terrorism or activities in preparation therefore" for purposes of the statute.[18] However, for reasons discussed in Section II, the nature of the current global terrorist threat does not easily conform to "agent of a foreign power" equivalence for these purposes.

Finally, FISA provides only a single cumbersome binary mechanism that requires an individual application to the Foreign Intelligence Surveillance Court ("FISC") for authorization to target a specific individual or communication to or from the United States based on an *pre hoc* showing of probable cause that the target is acting as an agent of a foreign power or foreign terrorist group,[19] but provides no mechanisms for authorizing

---

[17] 50 U.S.C. § 1805(a)(3)(A) (2000).

[18] 50 U.S.C. § 1801(a)(4) (2000). However, the prevailing paradigm of 'international terrorism' at the time that FISA was enacted generally consisted of isolated attacks conducted abroad against U.S. national interests. *See also* note 34 *supra.*

The definition of "agent of a foreign power" was further stretched in 2003 to include so-called "lone wolves." §1801(b)(1)(C). (The 'lone wolf' amendment is often referred to as the "Moussaoui fix." *See, e.g.*, Press Release, Office of Senator Charles E. Schumer, Schumer, Kyl to Introduce Moussaoui-fix, Jun. 5, 2002, *available at* http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/PR01025.html.

[19] In the case of a U.S. person, FISA requires probable cause to believe that the target is an "agent of a foreign power," 50 U.S.C. § 1801(b) and that the person's activities "involve or are about to involve" a violation of the criminal laws of the United States, § 1801(b)(2)(B); or are activities in preparation for sabotage or "international terrorism" on behalf of a foreign power, § 1801(b)(2)(C).

A court order authorizing electronic surveillance to target a specific person or communication for foreign intelligence purposes is sought under 50 U.S.C. § 1804 by application of a federal officer in writing on oath or affirmation to a FISC judge after approval by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 *et seq.* have been met. Section 1804(a) sets out specifically what must be included in the application and § 1805(a) sets out the findings and probable cause standards required of the FISC judge. Finally, § 1805(c) sets out the limitations that must be specified in the order.

In addition to the inflexibility of the FISA warrant procedures to accommodate the circumstances described later in this article, the efficacy of requiring traditional warrants in all cases for foreign intelligence surveillance was itself questioned by then Attorney General Edward Levi in 1975:

> Levi said … [f]oreign intelligence … may in some situations require "virtually continuous surveillance, which by its nature does not have specifically predetermined targets." In these situations, "the efficiency of a warrant requirement would be minimal."

John Schmidt, *A Historical Solution to the Bush Spying Issue*, CHIC. TRIB., Feb. 12, 2006. *See also Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence*, 109th Cong. (2006) (testimony of Judge Richard A. Posner) (questioning the relevance of the warrant requirement to certain aspects of foreign intelligence surveillance).

advanced technical methods (including those discussed in this article) to help identify such agents in the first place.

II. 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.[20] Rather, changing context requires reflective reexamination of 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 cannot simply abandon cherished values because maintaining them is difficult, neither can we simply resist change because it is uncomforting.

A. 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

[20] Thus, 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 without accountable patrons or other support infrastructure subject to sanction or retaliation. Even previously successful counterinsurgency strategies—for example, providing participatory political opportunities—will likely be ineffective against an enemy inherently opposed to rule through democratic structures. 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. For a discussion of strategic counterterrorism options, see generally BARD E. O'NEILL, INSURGENCY AND TERRORISM (2d. ed., rev'd, 2005); DANIEL BENJAMIN & STEVEN SIMON, THE NEXT ATTACK: THE FAILURE OF THE WAR ON TERROR AND A STRATEGY FOR GETTING IT RIGHT (2005). For a discussion of defensive strategies for homeland security, see generally MICHAEL D'ARCY, *ET AL.*, PROTECTING THE HOMELAND 2006/2007 (2006). For a discussion of the role of the U.S. intelligence system in counterterrorism, see generally RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM (2006).

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.[21] Organized groups of non-state actors now have the potential capacity[22] and capability[23] 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.[24] In simple terms, the threat to national security is no longer confined only to other nation states.[25]

---

[21] *See generally* Taipale, *Frankenstein*, *supra* note 7 at 129-35; and K. A. Taipale, *Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties*, *in* EMERGENT INFORMATION TECHNOLOGIES AND ENABLING POLICIES FOR COUNTER TERRORISM 442-43 (Robert Popp & John Yen eds., Jun. 2006).

[22] Technologically-enabled capacities include the use of so-called weapons of mass destruction (WMDs), including chemical, biological, and nuclear (CBN) 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 (in particular, Supervisory Control and Data Acquisition systems or SCADA). *See, e.g.,* Alan Joch, *Terrorists Brandish Tech Sword, Too*, FEDERAL COMPUTER WEEK, Aug. 28, 2006.

[23] Technologically-enabled capabilities include world-wide recruitment, organization, funding, planning, training, targeting, and command-and-control using global communication networks and the Internet. *See, e.g.,* Joch, *supra* note 22. In addition, these developments allow direct access to, or circumvention of, mainstream information distribution channels for propaganda purposes. For an overview of terrorist use of the Internet, see generally GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006) (see, in particular, the discussion of communicative uses of the Internet at 49-110; and instrumental uses at 111-46).

[24] In addition to the approximately 3,000 immediate deaths resulting from the terrorist attack on the World Trade Center 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 United States. 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.

[25] 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 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 377-94 (1999) ("Technology Goes International").

As Thomas Friedman writes in *The World is Flat*, 21st Century terrorism is the globalization of 20th Century terrorism.[26]

Thus, there has emerged a political consensus, at least with regard to certain threats, to take a preemptive rather than reactive approach.[27] "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."[28] 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[29]—but instead revolves around what methods are to be properly employed in this endeavor.

B. 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.[30] Since terrorist attacks at scales

[26] THOMAS FRIEDMAN, THE WORLD IS FLAT (2006). Globalized transnational terrorism, enabled and empowered in part by technology developments, *see* notes 22 & 23 *supra*, is simply qualitatively different than the then nascent "international terrorism" threat that was belatedly addressed in FISA by simply expanding the definition of "foreign power" to include "group[s] engaged in international terrorism" 50 U.S.C. § 1801(a)(4) (2000); *see also* note 18 *supra* and note 34 *infra*. *See generally* NETWORKS, TERRORISM AND GLOBAL INSURGENCY (Robert J. Bunker ed., 2005) (assessing the threat posed by global terrorism).

[27] 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), *available at* http://www.pbs.org/newshour/terrorism/international/fatwa_1996.html; Osama Bin Laden, *et al.*, *Jihad Against the Jews and Crusaders*, World Islamic Front Statement (1998), *available at* http://www.fas.org/irp/world/para/docs/980223-fatwa.htm. 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.

[28] 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 (2002).

[29] *See, e.g.*, *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before U.S. Senate Committee on the Judiciary*, 110th Cong. (2007) (statement of Sen. Edward Kennedy, Member, Comm. on the Judiciary) ("We all agree on the need for strong powers to investigate terrorism [and] prevent future attacks . . . .").

[30] Terrorism, by indiscriminately targeting civilians and infrastructure, limits the effectiveness of certain other counterstrategies that are otherwise useful, i.e., those useful against nation state adversaries conforming to the international laws of armed conflict

that can actually endanger national 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—actionable intelligence—so that additional law enforcement or security resources can then be allocated to such threats preemptively to prevent attacks.[31]

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.[32] 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."[33] "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.[34]

(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 against attack . . . ." MARKLE FOUNDATION, SECOND REPORT OF THE MARKLE TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE: CREATING A TRUSTED NETWORK FOR HOMELAND SECURITY 1 (2003) (arguing for improved information sharing in order to identify terrorists before they act).

[31] 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.

[32] *See, e.g.*, Adam Nagourney, *Seeking Edge In Spy Debate*, N.Y. TIMES, Jan. 23, 2006, at A1 ("'We all support surveillance . . . .' [Senator John] Kerry said."); Statement Released by U.S. Senator Patrick Leahy, Feb. 15, 2006, ("We all agree that we should be wiretapping al Qaeda terrorists . . . .").

[33] Richard A. Posner, *Commentary: A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16.

[34] 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 enacted to provide a statutory framework for the use of electronic surveillance within the United States of adversary nation state ("foreign power") espionage activities. *See generally, e.g.*, *Hearing on the Foreign Intelligence Surveillance Act H.R. 12750 before the Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the U. S. House of Representatives Committee on the Judiciary*, 94th Cong. (1976). Although FISA defines "group[s] engaged

C. 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[35] that moves easily across borders and hides among the general population, taking advantage of open societies to mask its own organization and activities.[36] 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.

---

in international terrorism" as "foreign powers" for purposes of the statute, 50 U.S.C. § 1801(a)(4) (2006), it simply did not contemplate the nature or scale of a globalized, non-state group conspiracy enabled by modern technology that could directly attack the U.S. homeland or generally threaten long-term national security, nor did it anticipate the need to use advanced technical methods to help identify and preempt such threats.

For a brief overview of the nature of modern terrorism see WEIMANN, *supra* note 23 at 20-23. In particular, see the discussion contrasting an intentionally oversimplified dichotomy of "old" and "new" terrorism, *id.* at 22, for which Weimann cites Shabtai Shavit, *Contending with International Terrorism*, 6 J. INT'L SECURITY AFF. 63-75 (2004) (proposing a permanent international mechanism to combat terrorism. *Id.* at 73-75).

[35] *See* bin Laden, *supra* note 27, and World Islamic Front Statement, *supra* note 27. *See also* Nassir bin Hamd al-Fahd, *Risalah fi hokum istikhdam aslihat al-damar al-shamel didh al-kuffar* (May 2003) (fatwa on the permissibility of WMD in jihad) *cited in* Robert Wesley, *Al-Qaeda's WMD Strategy After the U.S. Intervention in Afghanistan*, TERRORISM MONITOR, Vol. 3 Iss. 20, Oct. 21, 2005; CHRISTOPHER M. BLANCHARD, AL QAEDA: STATEMENTS AND EVOLVING IDEOLOGY (Congressional Research Service Report to Congress No. RL32759, 2007); ANONYMOUS, THROUGH OUR ENEMIES EYES at xii (2002) ("The United States is embroiled in a momentous struggle . . . . bin Laden . . . and . . . the movement he established is a foe that must be understood before his movement can be, and must be, defeated and eliminated").

[36] Although there is an ongoing global conspiracy hostile to U.S. interests with an identifiable core, the threat has metastasized to more autonomous and decentralized organizational structures creating additional challenges for security services. *See, e.g.*, *The Changing Face of Terror: A Post 9/11 Assessment*, *Testimony Before the Senate Committee on Foreign Relations by Ambassador Henry A. Crumpton, Coordinator for Counter-terrorism,* (Jun. 13, 2006) *available at* http://www.senate.gov/~foreign/testimony/2006/CrumptonTestimony060613.pdf. *See generally* DANIEL BENJAMIN & STEVEN SIMON, THE NEXT ATTACK (2005) ("Individuals who hitherto had no significant ties to radical organizations are enlisting themselves in the struggle and committing acts of violence, *sometimes without any support from existing networks*." (emphasis added) *id.* at xiii.) *See also* ANONYMOUS, *supra* note 35 at xii ("[T]he United States can no longer rely on its continental breadth, friendly neighbors, and broad oceanic shores to insulate it from [terrorist attack].").

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[37] attributes, such as citizenship, are technically impossible to enforce.

III. THE EAR OF DIONYSUS

The Ear of Dionysus (*L'Orecchio di Dionigi*) is the name given by the belligerently Baroque painter Caravaggio (1571-1610)[38] to a cave in Syracuse in which, legend has it, Dionysus[39] took advantage of the perfect natural acoustics that allowed eavesdropping on all conversations from one central spot.[40] *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.

A. FISA IS INADEQUATE

In addition to the general challenges detailed in the earlier section relating to preemption and the changed nature of the threat, 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:

---

[37] Here we mean *arbitrary* in a technical sense, that is, these attributes are unrelated to, or not obvious from, the data itself.

[38] Michelangelo Merisi da Caravaggio (b. Sep. 29, 1571 – d. Jul. 18, 1610) was an Italian artist considered the first great representative of the Baroque school. That he was belligerent is evidenced by a contemporary source: "[A]fter two weeks of work [Caravaggio] will sally forth for two months together with his rapier at his side and his servant-boy after him, going from one tennis court to another, always ready to argue or fight, so that he is impossible to get along with." CAREL VAN MANDER, HET SCHILDER-BOEK (1604), *translated in* HOWARD HIBBARD, CARAVAGGIO 344 (1985).

[39] 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).

[40] Dorte Zbikowski, *The Listening Ear: Phenomena of Acoustic Surveillance* in CTRL [SPACE]: RHETORICS OF SURVEILLANCE FROM BENTHAM TO BIG BROTHER 38 (Thomas Y. Levin, *et al.* eds., 2002).

- 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").[41]

- 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 surveillance or investigation to determine whether probable cause exists ("collateral intercepts"),[42] 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").

---

[41] *See* 50 U.S.C. § 1801 (f)(2) (2006); Eric Lichtblau & James Risen, *Domestic Surveillance: The Program; Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A6:

> 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.

see also note 42 *infra*.

[42] There is also a narrower but related problem where the incidental interception of international calls to or from the United States by a foreign surveillance target not normally subject to FISA are themselves viewed as triggering the warrant requirements of 50 U.S.C. § 1801(f)(2) when the interception is physically conducted from a switch in (thus, "occurs in") the U.S. It is believed that this was among the initial problems with FISA that lead to the Presidential authorization of the TSP, *see infra* text accompanying notes 54-61.

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

B. TRANSIT INTERCEPTS: FROM CIRCUIT-BASED TO PACKET-BASED COMMUNICATION NETWORKS

The fundamental architecture of modern communications networks has changed significantly since FISA was enacted requiring new methods to conduct electronic surveillance. These developments challenge existing constructs underlying electronic surveillance law and policy.

> 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 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.[43]

---

[43] K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance,* N.Y.U. REV. L. & SECURITY, NO. VII SUPL. BULL. ON L. & SEC.: THE NSA AND THE WAR ON TERROR (Spring 2006) (hereinafter "*Whispering Wires*") *available at* http://whisperingwires.info. The NSA itself has described these developments:

> In the past, NSA operated in a mostly analog world of point-to-point communications carried along discrete, dedicated voice channels. … Now, communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia. They are dynamically routed, globally networked and pass over traditional communications means such as microwave or satellite less and less. Today, there are fiber optic and high-speed wire-line networks and most importantly, an emerging wireless environment that includes cellular phones, Personal Digital Assistants and computers. … The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. … The volume, velocity and variety of information today demands [sic] a fresh approach to the way NSA has traditionally done business. … NSA's existing authorities were crafted for the world of the mid to late 20th Century, not for the 21st Century. … [Because of this new] communications environment … availability of critical foreign intelligence information will mean gaining access in new places and in new ways.

NATIONAL SECURITY AGENCY & CENTRAL SECURITY SERVICE, TRANSITION 2001 at 31-32 (Dec. 2000), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf.

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."[44] To intercept these kinds of communications, filters ("packet-sniffers")[45] and search strategies[46] 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.[47]

---

[44] JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 50 (2006)

[45] 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. For a readable technical discussion of sniffers, see SUMIT DHAR, SNIFFERS: BASICS AND DETECTION [v. 1.0-1] (2002), *available at* http://www.rootshell.be/~dhar/downloads/Sniffers.pdf.

[46] 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, search strategies covering multiple nodes (or covering multiple entry and exit points on proxy networks) may be needed to effectively intercept any particular communication. For a general discussion of proxy routing, including "mix networks" such as TOR that use "onion routing," see, Marc Rennhard & Bernhard Plattner, *Practical Anonymity for the Masses with Mix-Networks*, WETICE 255 (Twelfth International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003).

[47] A familiar example of a packet sniffing application for electronic surveillance was the Federal Bureau of Investigation's DCS-1000 application for lawful intercepts of email traffic (*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 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 certain details of the DCS-1000 remain classified, declassified documents describe 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. *See* Kevin Poulsen, *Carnivore Details Emerge*, SECURITYFOCUS, Oct. 4, 2000. 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 lawfully collected wiretap

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.[48] 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

information from an investigation of Osama bin Laden's terrorist network when the DCS application accidentally also intercepted and logged non-targeted communications. *Memo: FBI Destroyed Terrorism E-mails*, USA TODAY, Apr. 29, 2002, at A16.

It has recently been alleged that because of these technical limitations the FBI is now using a broader approach to lawful intercepts in which all traffic on a particular network segment is collected and then the data is 'filtered' after the fact to extract those messages subject to the particular warrant or court order. *See* Declan McCullagh, *FBI Turns to Broad New Wiretap Method*, CNET NEWS.COM , Jan. 30, 2007. Applicable law and policy simply must be updated to account for these technical realities and to incorporate procedures that recognize that technical limitations require new methods to accomplish appropriate and lawful uses.

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 under appropriate circumstances. However, existing laws and procedures, including those in FISA, are inadequate to accommodate technical and operational needs for their lawful employ while still protecting privacy and civil liberties.

[48] 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 White House Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence* (Dec. 19, 2005), http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html; and *Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act* (Dec. 21, 2005), http://www.dhs.gov/xnews/speeches/speech_0265.shtm.

without a warrant and there is no procedure within FISA that would accommodate this need.[49]

C. 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.[50] "In

---

[49] *See generally*, RISEN, *supra* note 44 at 42-60 (discussing the perceived need to circumvent FISA procedures); and *see* Eric Lichtblau & James Risen, *supra* note 41:

> 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 61 *infra* (discussing the FISC orders and speculating about the use of anticipatory warrants to 'pre-approve' certain collateral surveillance).

[50] 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 United States are—seem outdated as well. That place of collection and U.S. person rules are increasingly

fact, it is now difficult to tell where the domestic telephone system ends and the international network begins."[51] 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 consistent with FISA as currently constituted to engage in follow up electronic surveillance to determine if probable cause exists to target that individual,[52] even though the collateral intercept itself may give rise to a constitutionally reasonable suspicion.[53]

Communications of a U.S. person (including those to or from the United States) acquired incidental to a lawful foreign interception would generally be subject to collection, retention, and dissemination procedures

---

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 32-41 (2006) (advocating replacing place of collection and U.S. persons rules with an "authorized use" standard for information sharing).

[51] RISEN, *supra* note 44 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 even though the communication is in fact wholly foreign.

[52] 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 42 *supra* because they impose the same *a priori* requirements, that is, even in an 'emergency' situation FISA requires the Attorney General to 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 but triggers FISA).

[53] For an overview of the relevant 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.) *See also Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence,* 109th Cong. (2006) (testimony of Kim Taipale, Executive Director, Center for Advanced Studies in Sci. & Tech. Pol'y) (hereinafter, "*HPSCI Testimony*") (discussing general Fourth Amendment requirements at 7-10) **;** Taipale, *Frankenstein*, *supra* note 7 at 202-17 ("Towards a Calculus of Reasonableness"); K. A. Taipale, *Why Can't We All Get Along? How Technology, Security, and Privacy can Co-exist in the Digital Age*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED WORLD 151, at 171-78 (Jack Balkin, *et al., eds*., 2007) (discussing reasonableness and due process).

consistent with Executive Order 12,333.[54] While such information ostensibly 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 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 with other agencies for context) because it would be subject to minimization procedures that would prevent its further retention or dissemination. Further, if the collateral interception of a call to or from the U.S. occurred from a switch in the United States while conducting lawful foreign surveillance not otherwise subject to FISA, the incidental interception of that communication itself could be considered to trigger statutory FISA warrant requirements, thus, the collected information could not be used *even if it evidenced probable cause on its face* unless the original interception was somehow authorized.[55]

The problem is simply that FISA requirements are now being triggered by unanticipated circumstances for communications that were not originally intended to be subject to FISA (that is, those incidental to a legitimate foreign target intercept) because, among other things, 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 in this particular case 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 not be subject to FISA and might 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, any information from the collateral intercept could not be used in any manner (including especially for an application for a FISA warrant) if the incidental interception was deemed to have itself required a FISA warrant (because it occurred in the United States). Indeed, it appears that this specific "bootstrapping" problem was a particular concern of the FISC.[56]

Further, this problem could not simply be avoided by getting a FISA warrant for the original interception because it is uncertain whether the

---

[54] *See* note 15 *supra* and the referenced guideline documents.

[55] *See* 50 U.S.C. §1801 (f) (2000): "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).

[56] *See* Carol D. Leonnig*, Surveillance Court is Seeking Answers,* WASH. POST, Jan. 5, 2006, at A2 ("[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.").

FISC even has (or should have) jurisdiction[57] 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 in practice to meet the requirements to support a traditional FISA warrant application). Obviously, even if there were FISC jurisdiction, it would be impractical to obtain warrants covering all foreign intelligence targets on the supposition that they might initiate or receive a communication from within the United States.[58]

As described in media reports, it appears that the Terrorist Surveillance Program (TSP) was specifically intended to address a particular aspect of the collateral intercept problem—that is, to authorize surveillance of collateral communications to and from the U.S. intercepted incidental to legitimate foreign surveillance activity without a FISA warrant even where FISA statutory requirements might otherwise be triggered (for example, where the interception was physically conducted at a U.S. switch thus triggering § 1801(f)(2)). According to official statements, the TSP authorized interception of international communications under presidential authority where one party to the communication was a legitimate target of foreign intelligence surveillance even if the other party was in the United States or a U.S. person.[59] Such surveillance previously authorized under the TSP is now subject to the FISC orders:

> 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.[60]

---

[57] For a general discussion of the creation, membership, structure and jurisdiction of the FISC and FISCR, see CONGRESSIONAL RESEARCH SERVICE, THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW, (Congressional Research Service No. RL33833, Jan. 24, 2007).

[58] Note, however, that it may be precisely these circumstances that the FISC orders address through use of "anticipatory" warrants. *See* note 61 *infra*.

[59] Attorney General Gonzales has stated that: "the standard applied [in the NSA Terrorist Surveillance Program under Presidential authority]—'reasonable basis to believe' [that one party to the communication was 'terrorist']—is essentially the same as the traditional Fourth Amendment probable cause standard." Attorney General Alberto R. Gonzales, *Prepared Remarks at the Georgetown University Law Center* (Jan. 24, 2006), http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html, and, further, specifically stated that the current FISC orders are based on "probable cause" to believe that "one of the communicants is [a 'terrorist']." *See* Gonzales letter, *supra* note 2 and Transcript, *infra* note 82.

[60] Attorney General's letter, *supra* note 2.

It is unlikely that the original TSP or the new FISC 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.[61]

D. AUTOMATED ANALYSIS: CONTENT FILTERING, TRAFFIC ANALYSIS, AND LINK OR PATTERN ANALYSIS[62]

> 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.[63]

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

[61] Details of the FISC orders have not been publicly disclosed and the Justice Department has indicated that it is not prepared to release the orders to the public, *see* Government's Supplemental Submission, *supra* note 9 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 take the form of "anticipatory warrants" that would authorize surveillance in the future if certain factual predicates were to occur. Anticipatory warrants would require a judge to agree ahead of time that if certain facts were to occur at some point in the future (for example, if a legitimate foreign target were to communicate to or from the United States), then probable cause would exist at that time to justify surveillance and electronic monitoring would be authorized and could be carried out under the warrant. The use of anticipatory warrants was upheld in U.S. v. Grubbs, 126 S. Ct. 1494, 1500 (2006) (warrant containing "triggering conditions" is constitutional). Although the use of anticipatory warrants to authorize collateral intercepts in these circumstances would mitigate some aspects of the collateral intercept problem discussed in this article, an explicit statutory basis should be enacted to support such orders. On Feb. 27, 2007, the Electronic Frontier Foundation filed a Freedom of Information Act request seeking release of Department of Justice records relating to the FISC orders. EFF v. Department of Justice, No. 07-CV-00403 (D. D.C., filed Feb. 27, 2007).

[62] Parts of this subsection are adapted from Taipale, *Whispering Wires*, *supra* note 43.

[63] K. A. Taipale & James Jay Carafano, *Fixing Foreign Intelligence Surveillance*, WASH. TIMES, Jan. 25, 2006, at A15.

communications (or persons) of interest.[64] 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.[65]

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).[66] Traffic analysis can reveal patterns of organization, for example, by measuring "betweeness" in email traffic[67] 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.[68]

---

[64] For example, the Echelon program has been described as an NSA program (in partnership with corresponding agencies in Australia, Canada, New Zealand, and the UK) 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 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, 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 121-22.

[65] See discussion of link and pattern analysis below.

[66] *See* BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD 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").

[67] 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*, 40 SOCIOMETRY, Mar. 1977, at 35–41.

[68] 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*, 7 FIRST MONDAY, April 2002 (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 counterterrorism is focused on identifying unique characteristics of terror networks. *See generally* Philip Vos Fellman & Roxana Wright, *Modeling Terrorist Networks: Complex Systems at the Mid-*

These methods can uncover how terrorist groups are organized and reveal activity even if they are communicating in code or only discussing the weather.[69]

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.[70]

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 nineteen hijackers had made 206 international telephone calls to locations in Saudi Arabia, Syria, and Germany.[71] It is believed that in order to determine whether any other

---

Range, presented at Complexity, Ethics and Creativity Conference, London School of Economics (Sep. 17-18 2003); Joerg Raab & H. Briton Milward, *Dark Networks as Problems*, 13 J. OF PUB. ADMIN. RES. & THEORY 413-39 (2003); Matthew Dombroski *et al., Estimating the Shape of Covert Networks*, PROCEEDINGS OF THE 8TH INT'L COMMAND AND CONTROL RES. AND TECH. SYMPOSIUM (2003); H. Brinton Milward & Joerg Raab, *Dark Networks as Problems Revisited: Adaptation and Transformation of Islamic Terror Organizations since 9/11*, presented at the 8th Publ. Mgt. Res. Conference at the School of Policy, Planning and Development at University of Southern California, Los Angeles (Sep. 29-Oct. 1, 2005); D. B. Skillicorn, *Social Network Analysis Via Matrix Decomposition*, in EMERGENT INFORMATION TECHNOLOGIES AND ENABLING POLICIES FOR COUNTER TERRORISM (Robert Popp and John Yen, *eds*., Jun. 2006). For a general overview of global Salafi jihadist terror networks, *see* Marc Sageman, UNDERSTANDING TERROR NETWORKS (2004).

[69] *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 MAGAZINE, Mar. 12, 2006, at 16.

[70] 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 *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before U.S. Senate Judiciary Committee*, 110th Cong., at 6-16 (Jan. 10, 2007) (testimony of Kim Taipale, Executive Director, Center for Advanced Studies in Sci. & Tech. Pol'y) ("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.").

[71] John Crewdson, *Germany says 9/11 hijackers called Syria, Saudi Arabia*, CHI. TRIB., Mar. 8, 2006, at C17 ("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.").

unknown persons—so-called sleeper cells—in the United States might have been in communication with the same pattern of foreign phone numbers[72] the NSA analyzed Call Data Records (CDRs) of international and domestic phone calls obtained from the major telecommunication companies. [73] 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.[74]

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[75]

---

[72] That is, to uncover others who may not have a direct connection to the nineteen known hijackers but who may exhibit the same or similar *patterns of communication* as the known hijackers.

[73] That the NSA obtained CDRs from U.S. telecommunication carriers for analysis was implied in Lichtblau, *supra* note 41, and was explicitly alleged in Cauley, *supra* note 2.

[74] 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"), 50 U.S.C. § 1842 (2000), however, it provides no mechanism for authorizing searches for specific traffic information from general databases.

It is settled law under *Smith v. Maryland*, 442 U.S. 735 (1979), that addressing information is generally entitled to lesser constitutional protection than communication content. *See generally* ELIZABETH B. BAZAN *ET AL.*, GOVERNMENT ACCESS TO PHONE CALLING ACTIVITY AND RELATED RECORDS: LEGAL AUTHORITIES 3-5, (Congressional Research Service Report to Congress No. RL33424, 2007). 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. *See, e.g.*, United States v. Sokolow, 490 U.S. 1 (1989); Steven K. Bernstein, *Fourth Amendment: Using the Drug Courier Profile to Fight the War on Drugs*, 80 J. CRIM. L. & CRIMINOLOGY 996 (1990). More relevant, the court in *United States v. Lopez*, 328 F. Supp 1077, 1092 (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.

[75] *See, e.g.*, *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before the U.S. Senate Committee on the Judiciary*, 110th Cong. (Jan. 10, 2007) (testimony of Robert Barr, Chief Executive Officer, Liberty Strategies, LLC); and *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before the U.S. Senate Committee on the Judiciary*, 110th Cong. (Jan. 10, 2007) (testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute).

and civil libertarians[76] concerned about fishing expeditions or general searches to examine all communication flows in the manner of a general warrant.[77] 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 innocence.[78] 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.[79] As such, automated analysis is simply

---

[76] *See, e.g.*, *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before the U.S. Senate Judiciary Committee*, 110th Cong. (Jan. 10, 2007) (statement of Leslie Harris, Executive Director, Center for Democracy & Technology); *see* JAY STANLEY & BARRY STEINHARDT, AMERICAN CIVIL LIBERTIES UNION, BIGGER MONSTER, WEAKER CHAINS: THE GROWTH OF AN AMERICAN SURVEILLANCE SOCIETY 11-12, (2003).

[77] *See, e.g.*, Taipale, *HPSCI Testimony*, *supra* note 53 at 5-6 ("*Programs of surveillance* are not general warrants"). It was the use of general warrants by the English that led in part to the American Revolution, *see, e.g.*, O.M. Dickerson, *Writs of Assistance as a Cause of the Revolution*, in THE ERA OF THE AMERICAN REVOLUTION 40-75 (Richard Morris ed., 1939), and to enactment of the Fourth Amendment, *see* EDWARD CORWIN, THE CONSTITUTION AND WHAT IT MEANS TODAY at 341 (1978, 1920); DAVID HUTCHINSON, THE FOUNDATIONS OF THE CONSTITUTION at 294-95 (1975, 1928); *and* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION at 51-105 (1937).

[78] See *Connecting the Dots*, supra note 70 at 19; and Paul Rosenzweig, *Proposals for Implementing the Terrorism Information Awareness System*, 2 GEO. J. L. & PUB. POL'Y 169, 190 (2004) (discussing the appropriate consequences of pattern-based identification).

[79] One of the criticisms of using predictive risk management techniques for counterterrorism is to suggest 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 76 at 12; JEFF JONAS & JIM HARPER, CATO INSTITUTE, EFFECTIVE COUNTERTERRORISM AND THE LIMITED ROLE OF PREDICTIVE DATA MINING 7 (December 11, 2006) (for a detailed critique of the many inductive fallacies in the Cato Institute paper, *see* Testimony, *supra* note 70). But such an assumption is not uncritically warranted as these simplistic arguments confuse the use of probability-based resource allocation for investigative purposes with the assignment or determination of guilt (that is, they confuse attention with a determinative inference of "suspicion").

For example, in the ordinary course of law enforcement, the use of statistical or trend analysis to assign resources—say more beat officers to a high crime neighborhood—does not automatically lead to the inference that everybody in that neighborhood is a suspect, only that assigning resources there may be more effective than assigning them 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 or otherwise denying rights—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*, 20 IEEE INTELLIGENT SYSTEMS, Sept./Oct. 2005, at 80–83("[I]t is the probative value of the [analysis], rather than its probabilistic nature, that is relevant in determining

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 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. Simply to insist that these problems be ignored and that FISA is adequate "as is" is to engage in policy-making in a dangerous state of denial reminiscent of King Ludd.[80] Likewise, seeking solution only in streamlining cumbersome procedures[81] is to address symptoms, not root causes. Nor is it appropriate as a matter of public policy to resolve the deficiencies through "innovative" interpretations of existing FISA provisions, particularly when such outcomes are negotiated in secret and enacted through undisclosed FISC orders.[82] What is needed, in my view, is a rethinking of foreign intelligence

---

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).

[80] *See* Taipale, *Frankenstein*, at 126-27, 220-21 (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).

[81] For example, as proposed in the Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act ("LISTEN Act"), H.R. 5371, 109th Cong. (2006) (the Harman-Conyers bill) (providing tools to expedite emergency warrant applications and authorizing funds to incorporate standardization, electronic filing and streamlined review procedures at the NSA and DOJ for FISA warrant applications). These provisions are both laudable and necessary—but not alone sufficient. However, such procedural improvements should be included in any future legislation that also addresses the substantive failings of FISA as discussed in this article.

[82] 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":

> 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.

Transcript of Background Briefing by Senior Justice Department Officials on FISA Authority of Electronic Surveillance (Jan. 17, 2007), *available at* http://www.fas.org/irp/news/2007/01/doj011707.html.

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.[83]

IV. 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[84] without requiring individual warrants for *transit intercepts*, that is, intercepts "at the

---

But, "[t]he legality of this … surveillance program should not be decided by a secret court in one-sided proceedings." Press Release, American Civil Liberties Union, ACLU Demands More Information on "Innovative" Orders Issued by Secret Court, (Jan. 17, 2007). For speculation about the nature of the FISC orders, *see* note 61 *supra*.

[83] Despite the issuance of the FISC orders now authorizing surveillance previously authorized under the TSP, 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 82.

[84] It is beyond the scope of this article to recommend particular mechanisms or standards for authorizing programmatic or other 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. & Lee A. Casey, *Commentary: Inherent Authority*, WALL ST. J., Feb. 8, 2006, at A16 ("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, S. 3931, 109th Cong. (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, S. 3876, 109th Cong. (2006) (the Specter bill) that would require FISA court (FISC) approval and oversight, including review every forty-five days to continue "electronic surveillance programs." *See also*, Taipale, *HPSCI Testimony, supra* note 53 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.* Electronic Surveillance Modernization Act, H.R. 5825, 109th Cong. (2006) (the Wilson bill) (passed by the House on Sep. 28, 2006 and referred to the Senate Committee on the Judiciary) (requiring Congressional oversight but allow submission of the TSP to the FISC for review).

Although the exact scope of the current FISC orders has not been disclosed, the administration has denied that they are "programmatic" in the advisory sense:

switch" aimed at foreign communications but that might currently trigger statutory FISA warrant requirements[85] 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[86] without requiring individual warrants of *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,[87] and

3. the statutory equivalent of a *Terry* stop[88] to permit limited follow up electronic surveillance of suspicious communications, including those involving U.S. persons, *collaterally intercepted* incidental to an authorized surveillance (including incidental to those authorized through programmatic approval under (1) and (2) above).

> I will say that these are not – these orders are not some sort of advisory opinion ruling on the program as a whole. These are orders that comply with the terms and requirements of the FISA statute, just like other orders issued by the FISA court.

Transcript, *supra* note 82. Thus, it has been speculated that the orders are more in the nature of anticipatory warrants, *see* note 61 *supra*, that authorize surveillance when or if certain circumstantial facts that would amount to probable cause occur in the future. *See, e.g.*, *How Do Innovative Spy Warrants Work? One Expert Speculates*, WIRED News, Jan. 22, 2007, at 27B.

[85] Note that these are statutory warrant requirements, not Constitutionally requirements. *See* Taipale, *HPSCI Testimony*, *supra* note 53 at 8-9 (discussing warrant requirements). As discussed in note 15 *supra*, even under the stricter standard of Title III, the Supreme Court has repeatedly held that warrantless interceptions collateral to a lawful intercept are not violations of the Fourth Amendment.

[86] *See supra* note 84.

[87] Note that under some intelligence collection guidelines, electronic data is generally not considered "collected" until it has been processed into intelligible form. *See, e.g.*, Department of Defense Directive 5240.1-R *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 guidelines.

[88] 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).

It is beyond the scope of this article to examine the related constitutional jurisprudence in detail.[89] 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.[90]

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

[89] For a detailed discussion of the Constitutional issues involved, *see* references in note 53 *supra;* and RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY (2006).

[90] Note that with regard to the TSP, Attorney General Gonzales has stated that: "the standard applied—'reasonable basis to believe'—is essentially the same as the traditional Fourth Amendment probable cause standard." Gonzales, *supra* note 59. And, further, that the current FISC orders are based on "probable cause." *See* Gonzales letter, *supra* note 2 and Transcript, *supra* note 82. For an overview of the Fourth Amendment probable cause and reasonable suspicion standards, *see* Congressional Research Service Memorandum to the Senate Select Committee on Intelligence, *supra* note 53 at CRS-2 ("… 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.").

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 *ad hoc* anticipatory procedures, see note 61 *supra*) or a "shift-supervisor" [senior intelligence officer] at the NSA in "hot pursuit" of an intercepted communication—makes the determination. A statutory *Terry*-like procedure would address both by leaving some discretion with the "officer on the scene" (consistent with *Terry*) but subject to explicit statutory procedures and the Constitutional standard of reasonableness.

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.[91]

[91] Incidental intercepts of U.S. person data are subject to minimization procedures that in practice restrict effective use of such collateral information unless it has foreign intelligence or counterintelligence (or in some cases, criminal intelligence) value on its face. Use, retention or dissemination of such information is restricted by minimization guidelines—for example, by blocking out the name or phone number of U.S. persons (*see, e.g.,* USSID 18 §6(b): "may be disseminated … if the identity of the United States person is deleted and a generic term or symbol substituted so that the information cannot reasonably be connected with an identifiable United States person")—in a way that does not, in practice, permit it to be used to develop independent probable cause to target that U.S. person, particularly where its foreign intelligence value would only be apparent upon follow up investigation or dissemination. 50 U.S.C. § 1801 (h) (2000); *see* note 15 *supra* (Executive Order 12,333 and related guideline documents). (Prior to 9/11 such information was not even routinely shared with other government agencies and, in keeping with Attorney General guidelines, could not even be shared in practice within the FBI itself between the intelligence division and the criminal division. *See* Attorney General Janet Reno, Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations (Jul. 19, 1995). This latter problem was subsequently addressed in the Mar. 6, 2002 Attorney General guidelines, *Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI*.) And, as discussed in Section III (B) & (C) *supra*, in cases where the collateral intercept itself triggers FISA (because it "occurs in the United States," for example) such information cannot subsequently be used at all unless the original interception is specifically authorized. Indeed, it appears that concern specifically 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. Thus, another way to deal with this particular aspect of the collateral intercept problem would be to change the statutory minimization procedures to explicitly permit some limited follow-up investigation or surveillance (along the lines suggested above under the *Terry* stop equivalent) and to explicitly sanction the use of information gleaned during this period (or otherwise collateral to a programmatic intercept) for subsequent warrant applications.

It should be noted that Attorney General Gonzales in his testimony to the Senate Judiciary Committee on Jan. 17, 2007 specifically mentioned that the FISC orders include minimization procedures "above and beyond" those typically required under the law. Thus, it can be speculated that through a combination of anticipatory warrants (*see* note 61 *supra*) and enhanced minimization procedures, the administration and the FISC (or at least one judge of the FISC) were able to agree a procedure that authorizes collateral intercepts and permits information from those intercepts to act as predicate for limited targeting of international communications. Information collected pursuant to those orders could then presumably serve as the basis for requesting a 'normal' FISA warrant to target the domestic end or U.S. person should probable cause be established (indeed, the predicate for such targeting may have been already been predetermined as part of the "anticipatory warrants,"

The problem with FISA is that it contemplates only a single binary *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.[92] Unfortunately, even extensive contact with a known terrorist may not be procedurally sufficient to satisfy the current requirements for a FISA warrant, yet such contact 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 a statutory basis for the electronic surveillance equivalent of a *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.[93] 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[94]) 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

---

see note 61 *supra*). Again, the point of this article is to argue that FISA should be amended to provide an explicit statutory basis for these orders (or their equivalents).

[92] Assuming that the current FISC orders conform to the speculation regarding "anticipatory warrants," *see* note 61 *supra*, then what the administration and the FISC seem to have done is to have agreed a set of future factual circumstances that would amount to probable cause if (or when) they were to occur—that is, to anticipate that communications to or from a person in the United States with a legitimate foreign target may occur and to "pre-authorize" surveillance of those communications should they actually occur. While such a process might be shoehorned within the spirit and convoluted language of FISA, it would certainly have greater legitimacy—that is, a greater claim to be recognized as right and just, *see generally* Jurgen Habermas, COMMUNICATION AND THE EVOLUTION OF SOCIETY 178 (1976) (discussing "legitimacy")—if it were subject to explicit statutory authority and procedures. *See also* Schmidt, *supra* note 84 (arguing for legislation to explicitly extend the FISC jurisdiction to allow programmatic approval).

[93] *See* Taipale, *Whispering Wires*, *supra* note 43 (discussing the "electronic surveillance equivalent of a *Terry* stop").

[94] 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 would permit collateral intercepts and sanction 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 and manage disposition of collateral information. As discussed in note 91 *supra*, it appears that the FISC orders include enhanced minimization procedures.

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,[95] and that are currently being authorized under the FISC orders.[96]

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 central issue regarding 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 when the communication takes place within the United States. FISA currently provides no workable mechanism for addressing these circumstances and should be amended.

---

[95] *See, e.g.*, Remarks by Gen. Michael V. Hayden, Principal Deputy Director Of National Intelligence and Former Director of the National Security Agency*, Address To The National Press Club: What American Intelligence & Especially The NSA Have Been Doing To Defend The Nation*, National Press Club, Washington, D.C. (Jan. 23, 2006). (Gen. Hayden was subsequently appointed Director of Central Intelligence on May 8, 2006, confirmed by the Senate on May 26, 2006, and sworn in May 30, 2006).

[96] *See generally* notes 2, 42, 61, 82, 84, 90, 91, and 92 *supra*.