1 of 12 DOCUMENTS

Posner on In re: National Security Agency Telecommunications Records Litigation

2010 Emerging Issues 5030

Steve C. Posner on In re: National Security Agency Telecommunications Records Litigation (El Haramain Islamic Foundation, Inc v. NSA), 2010 U.S. Dist. LEXIS 31287 (N.D. Cal., Mar. 31, 2010), the Foreign Intelligence Surveillance Act and the State Secrets Privilege

By Steve Posner

May 3, 2010

SUMMARY: Although Congress has immunized telecommunications carriers from suit based on the NSA's domestic electronic surveillance program, the federal government remains a potential deep-pocket defendant. While it is difficult for a plaintiff to prove he or she was subjected to NSA surveillance and is an "aggrieved person," under FISA, the Al-Haramain Islamic Foundation has proved--at least pending appeal--that it is not impossible. Learn how they did it.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Since *The New York Times* reported in 2005 that the National Security Agency was conducting domestic electronic surveillance, dozens of plaintiffs have sued the federal government, federal officials, and the telecommunications companies that allegedly aided the government in violating the Foreign Intelligence Surveillance Act ("FISA"). Most of the lawsuits failed before the merit could be addressed, falling to the gauntlet of law, doctrine, and privilege raised by government defense attorneys. As an example of law, the 2008 FISA Amendments granted retroactive immunity to the telecommunications companies. Turning to doctrines, government lawyers asserted sovereign immunity. However, the most daunting challenge to plaintiffs has been the state secrets privilege (detailed in *Privacy Law and the U.S.A. PATRIOT Act*, § 4.44 *et seq.*), which the government has used either to dismiss cases on the ground that the very subject matter of the suit is a matter of national security, or to deny plaintiffs the evidence needed to make a *prima facie* case on the ground that disclosure would endanger national security.

Many of the NSA cases were consolidated under Judge Vaughn R. Walker of the U.S. District Court, Northern District of California. Among them has been *El Haramain Islamic Foundation, Inc v. NSA*, an action for money damages. What makes *Al-Haramain* different from other litigants n1 is that its plaintiffs successfully ran the gauntlet, at least at the trial level. n2

What makes this new *Al-Haramain* case particularly interesting has been the government's response once the Court ruled in 2008 that the state secrets privilege is subordinate to FISA and that Plaintiffs could amend their claim to allege facts independent of privileged evidence that could prove them "aggrieved persons" under FISA-that is, that Al-Haramain and the other Plaintiffs had been subjects of domestic electronic surveillance. (Under FISA, a plaintiff need not have been a target of such surveillance, but must merely have been subjected to it.)

The government refused to comply with court orders requiring the production of evidence to Plaintiffs' attorneys even after those attorneys were granted Top Secret clearance, continued to insist on arguments the Court had already dismissed, and continued to fight for immediate interlocutory appeal. The Court responded by offering Plaintiffs the option of sanctions precluding the government from contesting liability, or filing a summary judgment motion.

Plaintiffs filed the summary judgment motion. Pursuant to the Court's 2008 ruling that Plaintiffs could proceed if they assembled enough evidence to make a *prima facie* case of unlawful electronic surveillance that did not depend on privileged government evidence, Plaintiffs had busily assembled it. They had amended the claim to reflect their new independent evidence, and now they put it into their summary judgment motion.

Exasperated by such non-substantive government attempts to attack Plaintiffs' *prima facie* case as "their remarkable insinuation (unsupported by any evidence of their own) that the al-Buthi/al-Timimi intercepts might have been pursuant to a FISA warrant," the Court granted the motion based on the cumulative weight of the public evidence that:

- President George W. Bush had authorized the NSA to conduct domestic electronic surveillance of terrorist organizations related to al-Qaeda;
- The Treasury Department's Office of Foreign Asset Control has access to classified information sources when investigating terrorist financing;
- A Treasury Department official had testified to Congress in 2002 that Al-Haramain was a target of "Operation Green Quest," intended to track the financing of terrorist activities;
- The FBI's Terrorist Financing Operations Section ("TFOS"), which became the lead agency for the investigation of terrorist-related financial transactions, and acquired telecommunications of investigation targets for that purpose, took over the investigation of Al-Haramain;
- TFOS had access to Intelligence Community information. (The NSA is part of the Intelligence Community.);
- The FBI used the product of the NSA program;
- The FBI executed a search warrant on Al-Haramain's offices, and OFAC froze Al-Haraiman's assets, after the NSA program began and after OFAC sent Al-Haramain's lawyers a letter stating that Al-Haramain might be named a Specially Designated Global Terrorist based in part on classified information;
- An FBI official publicly acknowledged that the FBI had used "surveillance" in helping OFAC investigate Al-Haramain;
- Government officials had publicly acknowledged that most international communications are "wire communications" under FISA, and are subject to FISA if intercepted in the United States; and
- A Treasury Department memorandum publicly disclosed in a 2005 trial acknowledged electronic surveillance of an Al-Haramain employee's telephone conversations with the other individual plaintiffs.

Having awarded summary judgment on Al-Haramain's FISA claim, the Court offered Plaintiffs the choice seeking immediate entry of judgment on the FISA claim, or of pursuing their other claims.

Conclusion:

Although Congress has immunized telecommunications carriers from suit based on the NSA's domestic electronic surveillance program, the federal government remains a potential deep-pocket defendant. While it is difficult for a plaintiff to prove he or she was subjected to NSA surveillance and is an "aggrieved person," under FISA, *Al-Haramain* proves-pending appeal-it is not impossible.

Return to Text

n1 In a prior case in the Sixth Circuit, U.S. District Judge Anna Diggs Taylor, going straight to the merits,

ruled the NSA's domestic electronic surveillance illegal, only to be reversed on appeal based on the state secrets privilege. In *Al-Haramain*, the Court applied the court employed "the analysis and standard for establishing a prima facie case of electronic surveillance used by the Ninth Circuit in *United States v Alter, 482 F2d 1016 (9th Cir 1973)* (applying *18 USC § 3504(a)(1)*) and more recently by the DC Circuit in *In re Sealed Case (Horn v Huddle), 494 F3d 139, 377 U.S. App. D.C. 307 (DC Cir 2007/*." *In re: National Security Agency Telecommunications Records Litigation (El Haramain Islamic Foundation, Inc v. NSA*), *2010 U.S. Dist. LEXIS 31287*, *21-22 (N.D. Cal., Mar. 31, 2010).

n2 Detailed in the opinion and accompanying commentary to *Al-Haramain Islamic Foundation, Inc. v. Bush, 564 F. Supp. 1109 (N.D. Cal. 2008).*

RELATED LINKS: For more discussion of the state secrets privilege, see
- Privacy Law and the USA PATRIOT Act, Section 4.32

For discussion of terrorist designations and asset blockage, see generally
- Privacy Law and the USA PATRIOT Act, Chapter 3

For discussion of government tracking of financial transactions, see generally
- Privacy Law and the USA PATRIOT Act, Chapter 5

For discussion of information sharing among government agencies, see generally
- Privacy Law and the USA PATRIOT Act, Chapter 9

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise *Privacy Law and The USA PATRIOT Act* (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for *The Colorado Lawyer* magazine, and former co-chair of the Colorado Bar Association's Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

2 of 12 DOCUMENTS

Posner on Quon v. Arch Wireless Operating Co.

2010 Emerging Issues 4980

Steve C. Posner on the the architecture of government surveillance and the pending U.S. Supreme Court case of Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008), cert. granted, City of Ontario v. Quon, 175 L. Ed. 2d 617; 2009 U.S. LEXIS 9058 (2009) and cert. denied, USA Mobility

By Steve Posner

April 21, 2010

SUMMARY: When is notice to a government employee that an employer may conduct surveillance of employee communications sufficient under the Fourth Amendment? What are the Fourth Amendment privacy rights of third parties with whom the government employee has communicated? What federal statutory rights apply to communications of employees, employers, and service providers? The answers to any or all of these questions may be given in Quon.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Introduction:

On December 14, 2009, the United States Supreme Court granted certiorari and will review *Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008).*

Darrell VanDeusen has also written an analysis on this case, which can be found on Lexis at *2010 Emerging Issues 4837.* My perspective, focused as it is on post-9/11 national security, surveillance and privacy law, leads me to look at different issues. Each of our analyses, of course, may be mooted by the Supreme Court's decision in Quon.

Facts:

Mr. VanDeusen provides a capable and more extensive rendition of the facts than is provided here, where, for the reader's convenience, I state only the facts relevant to my analysis.

Quon was a police officer and SWAT team member employed by the City of Ontario, California ("Ontario"). He was issued a pager capable of text messaging. Ontario had no policy directed specifically at the pagers, but did have an employee manual prohibiting private use of city-owned computers and associated systems, reserving the right to monitor all network activity including e-mail and internet use, and stating that network access was not confidential. Quon acknowledged reading the manual. Ontario began issuing the pagers after Quon became employed, and after the manual was published.

Ontario had no official policy regarding pager use. It had an informal policy that if an employee's use exceeded what Ontario's service contract with Arch Wireless Operating Co. ("Arch Wireless") paid for, the employee would pay the overage. Police Lt. Duke, who oversaw the contract, told Quon that if he paid for the overages, his texting would not be audited. When Duke complained to Chief Scharf that he was tired of being a bill collector, Scharf told Duke to have Quon's messages audited to determine if they were work-related. Duke asked Arch Wireless for transcripts, and learned that Quon had exceeded his 25,000 character monthly allotment by more than 15,000 characters, and that many of the messages were personal, and some sexually explicit.

Quon, his wife, and other participants in the audited communications sued for, among other claims, violations of the Fourth Amendment and Stored Communications Act ("SCA"). The district court granted summary judgment to all defendants on the SCA claims, finding that Arch Wireless was a remote communications service ("RCS"), rather than an electronic communications service ("ECS"), under that law. According to the district court, the distinction between an ECS and an RCS is the central role that a computer plays in an RCS by providing remote long-term storage of communications, where such storage is not incidental to the transmission of the communications. This distinction was crucial because a remote communications service can provide communications contents to subscribers, such as the City, as well as parties to the communication. An electronic communications service can't.

The district court allowed the Fourth Amendment claims to stand, reasoning that Lt. Duke's statement to Quon that the City's policy would not be enforced gave rise to Quon's reasonable expectation of privacy. Whether the City violated Quon's rights would depend on whether the court found that the audit was for the purpose of seeing whether Quon was abusing the pager, or whether the purpose was to determine if Quon's legitimate business use exceeded the allotted 25,000 characters, in which case his monthly limit would be increased.

The Ninth Circuit partially reversed in *Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2009),* and its decision is one of the latest in a long chain of Fourth Amendment cases that decide what a "reasonable expectation of privacy" is, under particular circumstances.

Analysis:

The Fourth Amendment to the United States Constitution provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no warrants shall issue, but upon probable cause supported by oath or affirmation."

Most Fourth Amendment cases focus on whether the government has conducted an "unreasonable" search. The determination of reasonableness is in the hands of Congress and the courts. To oversimplify, the government is supposed to submit the reasons it wants to conduct a search to a judge or magistrate, who will issue a search warrant upon finding the search reasonable. A statute authorizing a type of search will greatly increase the odds that the judiciary will deem the requested search reasonable. As the law has evolved, certain searches or personal information disclosures authorized by Congress without the requirement of a warrant have been deemed reasonable by the courts. Limits remain, however, and an illegal or constitutionally unreasonable search triggers the protection of the Fourth Amendment, generally known as the "exclusionary rule." The welter of warrant requirement exceptions that has developed under statute and court doctrines has made this area of law quite confusing.

A subject that has been less examined is what does it mean when the exclusionary rule has been triggered? What is it that the government cannot do because it illegally obtained information? Although the term "exclusionary rule" was not used by the Supreme Court in this context until 1949 in *United States v. Wallace & Tiernan Co., 336 U.S. 793, 798, 69 S. Ct. 824, 827, 93 L. Ed. 1042, 1049 (1949),* the rule itself goes back at least to 1807 and its early formulations and applications were sweeping. As the Court found in *Ex Parte Bollman, 8 U.S. 75, 110, 2 L. Ed. 554, 566, 1807 U.S. LEXIS 369 (1807):*

All the facts necessary to constitute this probable cause must appear upon oath or affirmation. It is not necessary

indeed that there should be positive proof of every fact constituting the offence; but nothing can be taken into the estimate, when forming an opinion of the probability that the fact was committed by the person charged, but facts supported by oath or affirmation.

No belief of a fact tending to show probable cause, no hearsay, no opinion of any person however high in office, respecting the guilt of the person accused, can be received in evidence on this examination.

At its peak, between 1886 and the end of the Second World War, the scope of Fourth Amendment protection in the regulatory and criminal realms was broad. *Boyd v. United States, 116 U.S. 616, 6 S. Ct. 524, 29 L. Ed. 746 (1886),* held that the revenue laws could not be used to compel disclosure of self-incriminating documents. Nor could documents be seized without a judicially-issued warrant and laid before a criminal grand jury. The consequences of such a violation were drastic:

The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before a court but that it shall not be used at all. Of course this does not mean that the facts thus obtained become sacred and inaccessible. If knowledge of them is gained from an independent source they may be proved like any others, but the knowledge gained by the Government's own wrong cannot be used by it in the way proposed.

Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385, 392, 40 S. Ct. 182, 183, 64 L. Ed. 319, 322, 1920 U.S. LEXIS 1685 (1920), overruled, *United States v. Havens, 446 U.S. 620, 100 S. Ct. 1912, 64 L. Ed. 2d 559 (1980).* Nor could Congress, by statute, require businesses to provide the government with documents that could be used to incriminate them. See, e.g., *Stafford v. Wallace, 258 U.S. 495, 42 S. Ct. 397, 66 L. Ed. 735 (1922).* Similarly, if the government obtained communications information about a defendant in violation of Communications Act § 605, it was forbidden not only from introducing the exact words of the communication into evidence, but from derivative use of the illegally obtained information. "To forbid the direct use of methods thus characterized but to put no curb on their full indirect use would only invite the very methods deemed 'inconsistent with ethical standards and destructive of personal liberty.'" *Nardone v. United States, 308 U.S. 338, 340, 60 S. Ct. 266, 267, 84 L. Ed. 307, 311 (1939).*

After World War II, however, the Court began to chip away at the Boyd/Silverthorne doctrine, expressly overruling it in *United States v. Havens, supra.*

In criminal prosecutions, it allowed illegally obtained evidence to be used to impeach a criminal defendant's direct testimony. See *Walder v. United States, 347 U.S. 62, 74 S. Ct. 354, 98 L. Ed. 503 (1954).* Then, the Court allowed the government to use illegally obtained evidence to impeach a defendant's testimony on cross-examination, and that the impeachment evidence can be used as substantive evidence of guilt. See *United States v. Havens, supra.* Still, there remain, some limits: The government cannot however, use illegally obtained evidence to impeach defense witnesses other than a defendant. See *James v. Illinois, 493 U.S. 307, 110 S. Ct. 648, 107 L. Ed. 2d 676 (1990).*

Nardone v. United States, supra, has been limited so that while use of illegally obtained wiretap information is still prohibited, use of information "obtained indirectly as a result of illegal wiretaps" apparently is not, and if an illegal wiretap precipitates an investigation that produces evidence against a defendant, that evidence is admissible. See *United States v. Costello, 171 F. Supp. 10, 1959 U.S. Dist. LEXIS 3529 (D.N.Y. 1959).*

In the national security arena, the fall of the wall between intelligence and criminal investigations brought about by § 218 of the USA PATRIOT Act, has made the courtroom environment become ever less favorable to the criminal defendant. The problem is worsened if illegally obtained information can be fed into the Information Sharing Environment databases and communications systems being developed pursuant to the Information Sharing Environment, pursuant to § 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004, which, as a matter of technology, lets illegally obtained information to be accessed and shared across different levels of government, and used to start a Costello-type investigation years after it is obtained. Illegally obtained "electronic surveillance"

information is supposed to be subject to suppression upon the motion of an aggrieved person, or destroyed if information about a person with a reasonable expectation of privacy in the information is accidentally obtained. See *50 U.S.C. § 1806*. However, proving oneself an aggrieved party is difficult when faced with the government's assertion of the state secrets privilege in a proceeding under the Classified Information Proceedings Act.

Further, given the welter of constitutional doctrines, statutes, and common law holdings governing the privacy of electronic communications, how is an ordinary person to understand whether he or she has a reasonable expectation of privacy in a communication, when he or she has no way of knowing how, where, or how long it is stored, under what conditions an employer might decide to access it, or whether a message recipient's government employment status determines the privacy expectations of people who send the employee messages but have no knowledge of the government employer's policies, or have no knowledge of the different standards that apply to public and private employers. For example, the reasonable privacy expectations of both private and public sector employees are the same, and depend on the operational realities of the workplace. See *O'Connor v. Ortega, 480 U.S. 709, 717, 107 S. Ct. 1492, 1497, 94 L. Ed. 2d 714, 723 (1987).* However, only the public sector employer is constitutionally obligated to conduct a search that is reasonable at its inception. See, e.g., *Baggs v. Eagle-Picher Indus., Inc., 957 F.2d 268 (6th Cir. 1992); Ritchie v. Walker Mfg. Co., 963 F.2d 1119 (8th Cir. 1992); Mares v. Conagra Poultry Co., Inc., 773 F. Supp. 248 (D. Colo. 1991),* aff'd, *971 F.2d 492 (10th Cir. 1992).*

And now, at last, we come to *Quon*, and the Supreme Court decision to come. While courts typically consider the limited questions before them, the Supreme Court has the latitude to look more broadly at the effects their decisions are likely to have on society at large. Given the increasingly inclusive architecture of government surveillance, the ever-expanding potential for government abuse of communications information, and the difficulty of proving that it has been abused, the questions presented the Court might be viewed thus:

- As to the privacy expectations of a government employee: Should a government employer's official no-privacy policy that does not explicitly cover a government technology be held to supersede an unofficial policy that expressly addresses that technology?
- As to the privacy expectations of persons who communicate with government employees: Should such persons be held to waive their reasonable expectations of privacy because they communicate with a government employee whose communication device is issued by his employer? What if they don't know the employee works for the government? What if they know he works for the government, but don't know the government employer's policies? What if they don't know the employee is using a government-issued communication device?
- As to government employers: Should government employers be required to use less intrusive policies that meet their reasonable investigatory needs, rather than intrude into personal information that can be used to damage the parties to communications years later for reasons unrelated to the original investigation?

Conclusion:

Quon v. Arch Wireless Operating Co., Inc., presents, on the surface, questions relating to the reasonable privacy expectations of electronic communicants who communicate through the communications facilities of government employers, and when searches of such communications by government employers are constitutionally reasonable. However, Quon also concerns the less visible but profound issue of the uses to which illegally obtained communications information can be put, given the increasingly inclusive architecture of government surveillance, the ever-expanding potential for government abuse of communications information, and the difficulty of proving that it has been abused.

RELATED LINKS: For a more complete discussion of electronic communications, the Information Sharing Environment, and the architecture of government surveillance, see

- Privacy Law and the USA PATRIOT Act, Chapter 4;
- Privacy Law and the USA PATRIOT Act, Chapter 9

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests, and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes. He writes frequently online commentaries and blogs on emerging issues and litigation for LexisNexis.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Association's Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

Information referenced herein is provided for educational purposes only. For legal advice applicable to the facts of your particular situation, you should obtain the services of a qualified attorney licensed to practice law in your state.

3 of 12 DOCUMENTS

Posner on the Newly Developing Information Sharing Environment

2010 Emerging Issues 4847

Steve C. Posner on 6 U.S.C. § 485 and the Newly Developing Information Sharing Environment

By Steve Posner

February 1, 2010

SUMMARY: The Information Sharing Environment may be the most important development in privacy since Louis Brandeis developed the concept more than a century ago. Learn what it is, how it is intended to work, the extent to which privacy is being protected as the Environment is implemented, and what it all means for you and your clients.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: The legal transformation from a "need to know" to a "need to share" culture among criminal and intelligence investigation agencies came to full conceptual bloom with the Intelligence Reform and Terrorism Prevention Act of 2004 § 1016, codified at *6 U.S.C. § 485*, which, as amended by the National Transit Systems Security Act of 2007, n1 formally created the Information Sharing Environment. The concept was not altogether new; the term "information sharing environment" first appeared in a May 2001 congressional report concerning the vulnerability of Defense Department networks used to share sensitive law enforcement information in the war on drugs. n2 In April 2002, Senator Charles Schumer described the problem caused by lack of coordination among federal agencies as follows: n3

There are over 40 federal agencies charged with law enforcement and intelligence gathering. Our safety relies in good part upon each and every one of them. When the left hand does not know what the right hand is doing, you have got a problem. When you have 20 left hands and 20 right hands and none of them know what the other is doing, you have got a potential disaster in the making. That is what we are facing right now. The background of human defense is good information sharing and coordination between federal law enforcement and intelligence agencies.

However, not until the latter half of 2004 did the Information Sharing Environment begin to take its presently evolving form with consideration of its impact on privacy. Jim Dempsey, Executive Director of the Center for Democracy and Technology, gave the following testimony before the House Government Reform Committee: n4

The Gilmore Commission, chaired by former Virginia Governor Gilmore, reached the same conclusion. The TAPAC appointed -- the Technology and Privacy Advisory Committee appointed by Secretary Rumsfeld also stressed the importance of protecting privacy. And the Markle Task Force.

Part of the answer is in the technologies themselves. Anonymization technologies that will minimize the amount of

information that is collected, quality control measures, auditing trails to make sure that information is not being abused or misused or compromised, and also the policies. The wall is now down. No one is proposing re-erecting it. Intelligence agencies and law enforcement agencies are sharing information as they never did before. The government agencies have broad collection authority. There is really not any information that the government does not have the legal authority to get.

But the Privacy Act and our other rules are outdated. And the guidelines have not been put in place for this new information sharing environment. And these guidelines need not tie the hands of investigators and law enforcement and intelligence officials. In fact, the guidelines can empower the officials as well as constrain them, by telling them what is permissible and what they are authorized to do.

We will need oversight, both congressional and in the executive branch. This Congress was wise in creating a privacy officer and a civil rights and civil liberties officer when it created the Department of Homeland Security. Similar mechanisms need to be created for the new information sharing structures, but at the end of the day the oversight, accountability mechanisms will benefit both national security and civil liberties.

Well-implemented accountability need not impede intelligence operations. Checks and balances result in clear lines of responsibility, well-allocated resources, protection against abuse, and the ability to evaluate and correct past mistakes. As this Committee moves forward to implement the recommendations of the 9/11 Committee, the Center for Democracy and Technology and the members of the Markle Task Force are at your disposal to work with you and move forward in achieving our shared goals.

The Intelligence Reform and Terrorism Prevention Act was introduced on September 23, 2004. On December 7, 2004, Sen. Dick Durbin summarized its purpose: n5

I thought to myself after 9/11: How could we have reached the point where the FBI, our premier law enforcement agency, had computers that had no access to the Internet; did not have a means of transferring photographs over computers, they had to send them overnight express; basically had no word search? At the FBI? In the 21st century? And it was a fact.

And as I started to explore this, I found that there was a huge bureaucracy protecting this inefficiency. Turf battles. Who's going to decide which computers go where?

Well, we broke through those turf battles. And this legislation will establish an information-sharing environment so finally the computers can speak to one another, and finally we will have someone in charge of coordinating that sharing of information. That will make America safer.

And the second thing that I worked on that I feel very strongly about is a privacy and civil liberties board, recommended by the 9/11 Commission. It's important for us to remember that protecting America is essential, but we shouldn't secure our safety at the price of our freedom. And I think this independent board will go a long way to protecting our individual freedoms.

The Information Sharing Environment is defined in § 1016 of the Act. n6 Unlike PATRIOT Act § 905, § 1016 does not govern solely the use of criminal investigations passed to the Intelligence Community. Section 1016's broader purpose is described in its title: "Coordination with Non-Federal Entities; Inspector General, United States Secret Service, Coast Guard, General Provisions Information Sharing." It governs the sharing of all "terrorism information," the definition of which is similar but not identical to the definition in the PATRIOT Act § 905 guidelines:

(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to--
(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in

transnational terrorism;
(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
(iii) communications of or by such groups or individuals; or
(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(B) includes weapons of mass destruction information. n7

"Weapons of mass destruction information" is defined as: n8

information that could reasonably be expected to assist in the development, proliferation, or use of a weapon of mass destruction (including a chemical, biological, radiological, or nuclear weapon) that could be used by a terrorist or a terrorist organization against the United States, including information about the location of any stockpile of nuclear materials that could be exploited for use in such a weapon that could be used by a terrorist or a terrorist organization against the United States.

Congress appropriated $30 million annually for Fiscal Years 2008 and 2009 n9 to accomplish the following stated goals (and help address the issue of divided accountability):

- Establish an Information Sharing Council to assist the President in developing an Information Sharing Environment among federal, state and local agencies, and the policies to govern such sharing; n10
- Establish a program manager, who can be appointed and removed at presidential discretion, to work with the Information Sharing Council to manage the development of the information sharing effort;
- Establish an Information Sharing Environment, in which incompatibilities among investigatory agencies will be made transparent, and analysts at all levels of government will be able to quickly obtain information needed for investigations, n11 and develop a "culture of information sharing." n12

All this is to be done while protecting privacy and civil liberties by propounding, in conjunction with the Privacy and Civil Liberties Oversight Board ("PCLOB"), n13 guidelines for such protection in the use of the Information Sharing Environment. n14 PCLOB began in 2004 as an agency within the Executive Office of the President, but in 2007 it became an independent executive branch agency whose five members are appointed by the President and confirmed by the Senate. n15 It is tasked to work with DHS, state and local governments, manage regional, state and local fusion centers, and also to issue reports to Congress. n16 In January 2007, Lee Hamilton, one of the co-chairs of the 9/11 Commission, assessed PCLOB's effectiveness as follows: n17

It took a long time to get it into place. And once it got into place, it's taken a long time, it seems to me, to get itself organized. And I'm not aware -- I try to follow these things fairly carefully -- I'm not aware that they have really stepped in and challenged any agency on a civil liberties question. Maybe they have; I'm certainly not aware of it. Almost everything you do in homeland security has a civil liberties implication to it. And the people that have to take action are under a lot of pressure to take action, but they need to be checked. They need to be reviewed on the question of what it is they're doing. How does it impact on our privacy and on our civil liberties? We all understand the fact that we have lost a huge amount of civil liberty and a huge amount of privacy because of terrorism. You probably cannot avoid that; you certainly cannot avoid it completely. But you must have somewhere in the government a strong, robust review looking at every proposal that is made from a civil liberties standpoint. Now, we wanted an independent agency; we wanted a Senate confirmation; we wanted subpoena power; we wanted reports to the Congress regularly. I think most of that is in place -- maybe not the subpoena power -- but we have a board in place. And I think your function now is to make sure that that board is aggressive and robust in what they do. They have not been, I don't think up to this point, but they're still getting their act together.

PCLOB's budget for Fiscal Years 2008 and 2009 was $2 million annually, and it has not issued a report since Congress gave it independent status. n18

Subsequently, Executive Order 13,388 was promulgated to implement § 1016. n19 This order replaced E.O. 13,356, n20 which had sought to establish common standards for the "maximum distribution" n21 of terrorism information.

One interesting approach to developing common standards is that of the Department of Defense, which announced in December 2007 its plan to apply a generic "Blanket Routine Use" ("BRU") to every Privacy Act systems of records in DOD unless the systems notice for a particular system excludes use of the BRU. n22 The BRU is simple and broad: n23

A record from a system of records maintained by a [DOD] Component consisting of, or relating to, terrorism information (*6 U.S.C. 485(a)(4)*), homeland security information (*6 U.S.C. 482(f)(1)*), or Law enforcement information (Guideline 2 Report attached to White House Memorandum, "Information Sharing Environment," November 22, 2006) may be disclosed to a Federal, State, local, tribal, territorial, foreign governmental and/or multinational agency, either in response to its request or upon the initiative of the Component, for purposes of sharing such information as is necessary and relevant for the agencies to the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America as contemplated by the Intelligence Reform and Terrorism Protection Act of 2004 (Pub. L. 108-458) and Executive Order 13388 (October 25, 2005).

Conclusion:

As conceived, the Information Sharing Environment is the culmination of the fall of the "wall" between criminal and intelligence investigations begun by § 218 of the USA PATRIOT Act. It has the potential to be an intelligence/law enforcement tool, and an intrusion into personal privacy, unlike anything that has heretofore existed in the United States, because the priority and funding for the development of information sharing technology and procedures far exceeds that devoted to the protection of privacy rights. This Commentary is merely an introduction to this complex topic, which requires an examination of law, organization, systems, and privacy measures, as funded, planned, and implemented, across a large number of federal, state, local and tribal agencies. All practitioners who seek to protect clients from measures taken by the government under criminal, national security, financial, immigration, and employment law, and measures taken by the government under vague or non-existent legal authority, and those who administer the informational, institutional, and procedural systems that implement such measures, need to understand the developing Information Sharing Environment.

Return to Text

n1 Pub. L. No. 110-121, *121 Stat. 266.*

n2 Major General James Bryan, Commander Joint Task Force on Computer Network Operations (JTF/CNO Headquarters, U.S. Marine Corps (testimony before the House Armed Services Subcommittee on Military Readiness) (May 19, 2001).

n3 Sen. Charles Schumer (hearing before the Administrative Oversight and the Courts Subcommittee, Senate Judiciary Committee) (April 17, 2002).

n4 Jim Dempsey, Excutive Director, Center for Democracy and Technology (testimony before the House Government Reform Committee) (Aug. 3, 2004).

n5 Sen. Dick Durbin, (news conference) (Dec. 7, 2004).

n6 *6 U.S.C. § 485*.

n7 *6 U.S.C. § 485(a)(5)*.

n8 *6 U.S.C. § 485(a)(6)*.

n9 *6 U.S.C. § 485(l)*.

n10 *6 U.S.C. § 485(g)*.

n11 *6 U.S.C. § 485(b)*.

n12 *6 U.S.C. § 485(d)(3)*.

n13 Established at *5 U.S.C. § 601*.

n14 *6 U.S.C. § 485(d)(2)*.

n15 Pub. L. No. 108-458; see also, http://www.whitehouse.gov/administration/eop/pclob/; Harold C. Relyea, Congressional Research Serv, Order Code RL34385, Privacy and Civil Liberties Oversight Board: New Independent Agency Status (Updated Nov. 26, 2008), available at http://fas.org/sgp/crs/misc/RL34385.pdf.

n16 Id. For additional discussion of fusion centers, please see § 4.08 of Posner, Privacy Law and the USA PATRIOT Act (LexisNexis).

n17 Lee Hamilton, Co-Chair, 9/11 Commission (testifying before the Senate Homeland Security and Governmental Affairs Committee) (Jan. 9, 2007).

n18 C.R.S. Relyea report. At CRS-9.

n19 *70 Fed. Reg. 62,023.*

n20 *69 Fed. Reg. 53,599.*

n21 E.O. 13,388, § 3.

n22 Privacy Act of 1974; System of Records, *72 Fed. Reg. 73,781* (notice, Dec. 28, 2007).

n23 Id.

RELATED LINKS: For more discussion of the law underlying the Information Sharing Environment, see
- Privacy Law and the USA PATRIOT Act, Sections 9.01-9.21

For more discussion of the systems underlying the Information Sharing Environment, see
- Privacy Law and the USA PATRIOT Act, Sections 9.22 et seq.

For more discussion of the means by which the government gathers communications and movement information about individuals and entities since enactment of the USA PATRIOT Act, see generally

- Privacy Law and the USA PATRIOT Act, Chapter 4

For more discussion of the effects of the developing Information Sharing Environment upon those subject to immigration law, see generally

- Privacy Law and the USA PATRIOT Act, Chapter 6

For more information on new crimes and criminal prosecution of individuals and entities designated as terrorist, see generally

- Privacy Law and the USA PATRIOT Act, Chapter 8

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Association's Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

4 of 12 DOCUMENTS

Posner on Herring v. United States, 129 S.Ct. 695 (2009)

2009 Emerging Issues 3647

Steve C. Posner on Herring v. United States, the Exclusionary Rule, and the USA PATRIOT Act "Fall of the Wall"

By Steve Posner

February 6, 2009

SUMMARY: *Herring v. United States, 129 S. Ct. 695 (2009),* represents a sea change in Fourth Amendment and Exclusionary Rule jurisprudence by taking account of the mental state of police when a search or seizure is objectively unreasonable due to police record-keeping errors, and holding that the mental state must exceed mere negligence. It will change the ways in which Fourth Amendment challenges must be raised. Learn how.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: There was a time that the exclusionary rule could be simply stated: "In Weeks v. United States, supra, this Court held that in a federal prosecution the Fourth Amendment barred the use of evidence secured through an illegal search and seizure." n1 If a warrant was required under the Fourth Amendment, and the requirement was not met, then the requirement mandated suppression of the illegally obtained evidence, unless a search warrant exception n2 applied.

In *Herring v. United States*, n3 the United States Supreme Court made what appears to be a fundamental shift in exclusionary rule analysis, by holding that a Fourth Amendment violation does not necessarily trigger the rule if the underlying police error was merely negligent and not sufficiently deliberate that exclusion of evidence could meaningfully deter it. Unlike any prior warrant requirement exception case, *Herring* removes the exclusionary rule's incentive for the police to avoid negligence in carrying out searches and seizures. After *Herring*, the exclusionary rule applies only to serve "to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Herring* largely eviscerates a prior policy statement by the U.S. Supreme Court in *Michigan v. Tucker:* n4

The deterrent purpose of the exclusionary rule necessarily assumes that the police have engaged in willful, or at the very least negligent, conduct which has deprived the defendant of some right. By refusing to admit evidence gained as a result of such conduct, the courts hope to instill in those particular investigating officers, or in their future counterparts, a greater degree of care toward the rights of an accused.

Herring represents a policy decision by the Court that convicting criminals is more important than preventing citizen victimization due to police negligence in record keeping, unless such errors are shown to be so widespread or systemic that police would be reckless in relying on the particular database at issue.

Justice Ginsburg's dissent, joined by Justices Stevens, Souter, and Breyer, warns: n5

In light of the paramount importance of accurate recordkeeping in law enforcement, I would answer yes, and next explain why, as I see it, Herring's motion presents a particularly strong case for suppression.

Electronic databases form the nervous system of contemporary criminal justice operations. In recent years, their breadth and influence have dramatically expanded. Police today can access databases that include not only the updated National Crime Information Center (NCIC), but also terrorist watchlists, the Federal Government's employee eligibility system, and various commercial databases. *Brief for Electronic Privacy Information Center (EPIC) et al. as Amicus Curiae 6*. Moreover, States are actively expanding information sharing between jurisdictions. *Id., at 8-13, 115 S. Ct. 1185, 131 L. Ed. 2d 34*. As a result, law enforcement has an increasing supply of information within its easy electronic reach. *See Brief for Petitioner 36-37*.

The risk of error stemming from these databases is not slim. Herring's amici warn that law enforcement databases are insufficiently monitored and often out of date. *Brief for Amicus EPIC 13-28*. Government reports describe, for example, flaws in NCIC databases, 3 terrorist watchlist databases, and databases associated with the Federal Government's employment eligibility verification system.

The dissent's concern is underscored by a February 5, 2009 *New York Times* report on a National Academy of Sciences report expected to be published in February 2009. The *Times* reports that those who have seen the study say it is "is a sweeping critique of many forensic methods that the police and prosecutors rely on, including fingerprinting, firearms identification and analysis of bite marks, blood spatter, hair and handwriting." It can be inferred that if forensic methodology is systemically flawed, then the databases on which police and prosecutors rely also are systemically flawed in terms of the accuracy and reliability of the evidence they produce. As former-Justice O'Connor recognized in *Arizona v. Evans*, n6

In recent years, we have witnessed the advent of powerful, computer-based recordkeeping systems that facilitate arrests in ways that have never before been possible. The police, of course, are entitled to enjoy the substantial advantages this technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities.

Herring itself recognizes that, "[i]n a case where systemic errors were demonstrated, it might be reckless for officers to rely on an unreliable warrant system." n7

The *Herring* dissent also observed, "It is not clear how the Court squares its focus on deliberate conduct with its recognition that application of the exclusionary rule does not require inquiry into the mental state of the police." n8

After *Herring*, the practitioner who seeks to suppress evidence based on a police record-keeping error, or any issue involving a law enforcement database, should consider whether to subpoena or otherwise discover the entire police file and review it for evidence of record-keeping errors, in order to prove that police who rely on that database are reckless. As a practical matter, and as recognized by the *Herring* dissent, this is an expensive proposition that impoverished defendants may not be able to afford, and when a defendant *can* afford it, production and audit of police databases will be burdensome on police and the courts, and will be opposed on that basis. Opposition to production is likely to be still more vehement if the database at issue is one of the intelligence-related databases that have come into existence as a consequence of the USA PATRIOT Act. Such discovery battles, including possible invocations of the state secrets and National Security Act privileges, seem likely because PATRIOT Act § 218, which mandated the "fall of the wall" between intelligence and criminal investigation, opened the door to the use of more intelligence investigation information in criminal prosecutions, n9 and increased the need of criminal defendants to inspect the databases from which such information comes.

Herring v. United States represents a sea change in Fourth Amendment and Exclusionary Rule jurisprudence by taking account of the mental state of police when a search or seizure is objectively unreasonable due to police

record-keeping errors, and holding that the mental state must exceed mere negligence. Counsel challenging such errors may be compelled to subpoena or discover the erroneous databases to prove systemic error such that police reliance on the databases amounts to recklessness-an expensive and burdensome proposition for defendant and law enforcement alike. Since USA PATRIOT Act § 218 allows increased use of intelligence information in criminal prosecutions, the databases at issue may be sensitive, and discovery may be challenged on national security grounds. In turn, we may see more defense counsel using FISA evidence suppression provisions to challenge evidence offered by prosecutors.

Return to Text

n1 *Wolf v. Colorado, 338 U.S. 25, 29; 69 S. Ct. 1359, 1362; 93 L. Ed. 1782, 1786 (1949).*

n2 See *Privacy Law and the USA PATRIOT Act* § 2.04[3].

n3 *129 S.Ct. 695 (2009).*

n4 *417 U.S. 433, 447; 94 S. Ct. 2357, 2365; 41 L. Ed. 2d 182, 195 (1974).*

n5 *129 S.Ct. at 708.*

n6 *514 U.S. 1, 17; 115 S.Ct. 1185; 131 L. Ed. 2d 34 (1994).*

n7 Id.

n8 Id., *citing to Whren v. United States, 517 U.S. 806, 812-813, 116 S. Ct. 1769, 135 L. Ed. 2d 89 (1996).*

n9 Pub. Law 107-56 at § 218; *In re Sealed Case No. 02-001, 310 F.3d 717, 733 (FISA Ct. Rev. 2002).* For more discussion of the state secrets privilege, *see* § 4.44 of Privacy Law and the USA PATRIOT Act. For more

discussion of privilege under the National Security Act, *see* § 4.45 of Privacy Law and the USA PATRIOT Act.

RELATED LINKS: For more discussion of Fourth Amendment warrant exceptions, see
- 1-2 Privacy Law and the USA PATRIOT Act 2.04[3]

For more discussion of the state secrets privilege, see
- 1-4 Privacy Law and the USA PATRIOT Act 4.32

For more discussion of privilege under the National Security Act, see
- 1-4 Privacy Law and the USA PATRIOT Act 4.33

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise *Privacy Law and The USA PATRIOT Act* (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for *The Colorado Lawyer* magazine, and former co-chair of the Colorado Bar Association's Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

Posner on United States v. Alvarez-Machain

2008 Emerging Issues 2546

Steve C. Posner on United States v. Alvarez-Machain, 504 U.S. 655, 112 S. Ct. 2188, 119 L. Ed. 2d 441 (1992)

By Steve C. Posner

July 29, 2008

SUMMARY: Alvarez-Machain limited the circumstances under which U.S.-influenced acts could bring a foreign national within U.S. jurisdiction for trial, thereby setting the stage for the post-9/11 extraordinary rendition cases. Is it possible anymore for the government to go too far? Understand this complex evolving area, and protect your clients.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Cite as: Posner, Steve C. *United States v. Alvarez-Machain*. LexisNexis Expert Commentary, *(Insert date you accessed the document online).*

Extraordinary rendition has come to be understood as the secret transport of persons in U.S. custody to nations where they can be harshly interrogated. However, prior to the attacks of September 11, 2001, rendition dealt with bringing persons *into* the United States for trial. In *United States v. Alvarez-Machain*, the United States Supreme Court approved such conduct.

Alvarez-Machain, a Mexican citizen, was kidnapped from Mexico by Mexican nationals acting for the U.S. Drug Enforcement Agency and brought to the United States. Alvarez-Machain contended that his kidnapping violated the Extradition Treaty n1 between the two countries. The federal trial court held that the kidnapping violated the treaty and, therefore, the court lacked jurisdiction to try the defendant, and the Ninth Circuit Court of Appeals affirmed. The Supreme Court reversed, holding that, even though the kidnapping may have violated the general principle of international law that one state may not exercise its police power on the territory of another, the Extradition Treaty itself did not prohibit such a violation. Additionally, the mere fact that a defendant was brought to the U.S. by forcible abduction does not divest a U.S. court from the jurisdiction to try him. This was not the first time the Supreme Court approved hauling a defendant into a U.S. court by forcible abduction. In *Ker v. Illinois, 119 U.S. 436, 30 L. Ed. 421, 7 S. Ct. 225 (1886),* the Court approved a kidnapping in Peru. In *Ker*, it was not U.S. agents who had done the kidnapping, but although the trial and appellate courts in *Alvarez-Machain* found this difference dispositive, the Supreme Court did not. Alvarez-Machain stood trial.

Subsequently, he sued the Mexican nationals who had kidnapped him under the Alien Tort Statute, n2 and sued the United States under the Federal Tort Claims Act. He won judgment against the Mexican nationals but his FTCA claim was dismissed by the trial Court. The Ninth Circuit affirmed the ATS judgment but reversed the FTCA dismissal and

remanded. *See Alvarez-Machain v. United States, 331 F.3d 604 (9th Cir. 2003).* The U.S. Supreme Court reversed and remanded in *Sosa v. Alvarez-Machain, 542 U.S. 692, 124 S. Ct. 2739; 159 L. Ed. 2d 718 (2004),* holding that the FTCA did not apply because the claim arose in a foreign country, and the ATS did not apply because Alvarez-Machains brief detention (less than one day) by the Mexican nationals did not amount to a violation of a well-defined norm of customary international law, which the court held limited to the handful of international law *cum* common law claims understood in 1789 *(542 U.S. at 730*)--violations of safe conduct or the rights of ambassadors, and piracy. (A finding seemingly at odds with the Courts 1992 comment that the kidnapping might have been shocking and in violation of general international law principles. *112 S. Ct. 2188, 2197*.)

Since *Sosa*, it has been held that even if U.S. agents are in the foreign country, coordinating with the indigenous police at the time of the kidnapping, the FTCA does not apply; only if the U.S. agents do the kidnapping or arresting themselves does the FTCA govern. *See United States v. Bourdet, 477 F. Supp. 2d 164 (D. D.C. 2007)* (citing *22 U.S.C. § 2291*(c)(1) and (2), which govern the actions of U.S. agents on foreign soil).

Alvarez-Machain was also cited to justify (1) the trial of former Panamanian President Manuel Noriega, who was apprehended by U.S. forces and brought to the United States after declaring war between the U.S. and Panama (s*ee United States v. Noriega, 117 F.3d 1206 (11th Cir. 1997));* and (2) the apprehension on the high seas, on a foreign-flagged vessel, of a ship captain accused of alien smuggling (s*ee United States v. Best, 304 F. 3d 308 (3rd Cir. 2002)).*

The *Alvarez-Machain* line of cases intersected the post-9/11 rendition cases in *Khaled El-Masri v. Tenet, 437 F. Supp. 2d 530 (E.D. Va. 2006),* in which a German citizen claimed to have been kidnapped by the United States and shipped overseas to be tortured. He brought suit under, among other theories, the Alien Tort Statute, arguing that under *Alvarez-Machain*, he was entitled to sue for a violation of well-established international law. *Alvarez-Machain* did not govern *El-Masri*, which was dismissed as barred by the governments assertion of state secrets privilege. However, had the privilege not applied, the Court might well have dismissed *El-Masri* on the ground that extraordinary rendition, like the kidnapping in *Alvarez-Machain* was not a claim recognized in 1789 and, therefore, not actionable under the ATS.

Conclusion. What limits apply, then, to overseas kidnapping, arrest, or rendition by the U.S. government? Government agents cannot directly make an overseas arrest. *See 22 U.S.C. § 2291*(c)(1). That said, mere illegal action by U.S. agents is not sufficient to divest a U.S. court of jurisdiction. *See United States v. Bin Laden, 156 F. Supp. 2d 359 (S.D. N.Y. 2001).* Only when the court obtained jurisdiction as the result of the government's deliberate, unnecessary and unreasonable invasion of the accused's constitutional rights does the court lose jurisdiction. *Id. at 275*. The view of what constitutes such an invasion has changed dramatically in the past 30 years. *Compare United States v. Toscanino, 500 F.2d at 275 (2nd Cir. 1974):*

[W]hen an accused is kidnapped and forcibly brought within the jurisdiction, the court's acquisition of power over his person represents the fruits of the government's exploitation of its own misconduct. Having unlawfully seized the defendant in violation of the Fourth Amendment, which guarantees "the right of the people to be secure in their persons . . . against unreasonable . . . seizures," the government should as a matter of fundamental fairness be obligated to return him to his *status quo ante*.

Moreover, under *Alvarez-Machain* and *Sosa*, even a gross government invasion of civil rights might not matter if the violation occurs in a foreign locale and is one of the limited international law *cum* common law claims understood in 1789.

Cross-references

For a more complete discussion of extraordinary rendition, *see Privacy Law and the USA PATRIOT Act, § 6.09*.

For more complete discussions of the state secrets privilege, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 2, 4, 6, and 9.

For more complete discussions of searches and seizures, *see generally Privacy Law and the USA PATRIOT Act*, Chapters 2 and 4.

Return to Text

n1 . Extradition Treaty, May 4, 1978, [1979] United States-United Mexican States *(31 UST 5059*, TIAS No. 9656).

n2

[2]. Also known as the Alien Tort Claims Act.

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

6 of 12 DOCUMENTS

Steve C. Posner on El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007)

2008 Emerging Issues 2534

Steve C. Posner on El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007): The State Secrets Doctrine and Extraordinary Rendition

By Steve C. Posner

July 16, 2008

SUMMARY: *Posner on El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007)* As the war on terror moves the nation into uncharted legal territory, El-Masri and a growing body of cases raise important and fascinating issues concerning the state secrets privilege. Understand this complex evolving area, and protect your clients.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Cite as: Posner, Steve C. *El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007):* The State Secrets Doctrine and Extraordinary Rendition. LexisNexis Expert Commentary, *(Insert date you accessed the document online)*.

El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007), is one of a recent series of federal cases addressing the effect of the state secrets doctrine on extraordinary rendition cases.

Extraordinary Rendition. Extraordinary rendition is the capture and transfer of a person from one nation to another for legal or political purposes. Although originally used to describe the capture of a person overseas in order to bring that person to the United States for prosecution, under the George W. Bush Administration, the term has also been used to describe the detention of a person, and transfer of that person to the custody of an allied regime for interrogation that may involve torture. In the past few years, several plaintiffs have sued, alleging that they have been extraordinarily rendered and tortured.

State Secrets Privilege. The state secrets privilege is a common law evidentiary privilege that allows the government to deny discovery of military secrets. Assertion of this privilege, if upheld by the courts, can deny a plaintiff legal recourse for government abuses in two ways:

(1) If the very subject matter of the suit is a state secret, the suit must be dismissed without reaching any questions of evidence. The case is non-justiciable in a way similar to a political question.

(2) Assuming that the subject matter of the suit is found justiciable, denial of discovery may prevent the plaintiff from being able to prove either standing or a *prima facie* case, requiring dismissal.

Jurisdictional Conflict. *El-Masri* is remarkable in that it collapsed these two analytical steps into one by holding if

a case cannot be litigated without state secrets privileged information, this renders the very subject matter of the action a state secret. The Ninth Circuit, in the more recent case of *Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190 (9th Cir. 2007),* rejected the idea that the very subject matter of a suit and the facts needed to litigate are one and the same. *Id. at 1201*. The Ninth Circuits decision was similar to In re: *Sealed Case, 494 F.3d 139 (D.C. Cir. 2007)* (holding that Plaintiff had enough evidence independent of state secrets privileged information to make out a prima facie case). However, it is *Al-Haraiman* and *El-Masri* that crystallize what is now a jurisdictional conflict, because *El-Masri* explicitly equates the very subject matter and central facts of a lawsuit, and *Al-Haraiman* rejects that equation.

From a procedural point of view, the difference may be that, in the Fourth Circuit, a case necessarily involving privileged evidence may be dismissed in the context of a motion to dismiss. Arguably, in the Ninth and D.C. Circuits, such a case may survive a motion to dismiss but not survive a motion for summary judgment on evidentiary grounds.

It was perhaps with this in mind that in *Mohamed v. Jeppesen Dataplan, 2008 U.S. Dist. LEXIS 25940* (N.D. Cal. Feb. 13, 2008), the government moved to dismiss or, in the alternative, for summary judgment. However, the significance of the split in jurisdictions is questionable. In *Mohamed v. Jeppesen Dataplan, supra,* the district court gave lip service to *Al-Haraiman* but then granted the governments motion to dismiss on evidentiary grounds.

Subject Matter of a State Secret Case. When, then, is the very subject matter of a case of a state secret? It is a difficult question, because according to *Al-Haraiman* at 1200, courts are sometimes purposefully vague about the facts on which they base decisions. One can, however, anticipate that if the suit concerns weapons systems programs, covert overseas programs, or the involvement of identifiable persons or entities with such programs, the very subject matter is likely to be deemed a state secret and the case will probably be dismissed. Even if the very subject matter is not deemed a state secret in cases of identifiable involvement, dismissal is likely under a companion doctrine derived from *Totten v. United States, 92 U.S. 105, 23 L. Ed. 605 (1876),* which prohibits suits against the government based on covert espionage agreements. *See e.g., Tenet v. Doe, 544 U.S. at 11; 125 S. Ct. 1230, 1238; 161 L. Ed. 2d 82 (2005)* (The possibility that a suit may proceed and an espionage relationship may be revealed, if the state secrets privilege is found not to apply, is unacceptable); *see also (Valerie Plame) Wilson v. (Scooter) Libby, 498 F. Supp. 2d 74 (D. D.C. 2007).*

A related question is the effect of public disclosure of such a program. In *Hepting v. AT & T Corp., 439 F. Supp. 2d at 993 (N.D. Cal. 2006),* the court based its analysis on whether there was sufficient disclosure by reliable sources so that the NSA domestic electronic surveillance program, or at least aspects of it, could no longer be considered state secrets. However, in *Mohammed, supra,* the same court relied on *Al-Haraiman* for the precept that the privilege belongs to the government, and only government disclosure matters; disclosure by other reliable sources was held irrelevant. The *Mohammed* interpretation of *Al-Haraiman* was not necessarily sound, however. In *Al-Haraiman*, there were so many government disclosures, that reliance on other reliable sources was unnecessary; *Al-Haraiman* did not address reliable sources at all.

Conclusion. The law pertaining to the state secrets privilege is rapidly evolving, as numerous factors such as the degree of deference due the Executive Branch, the nature of intrinsically secret subject matter, the effects of public disclosure, the roles of involved individuals and entities, and the privileges relationship with related bodies of law, are discussed. Counsel dealing with extraordinary renditions, or other fact patterns regarding which the government has asserted or may assert the privilege, should perform a careful fact-specific assessment of the likelihood that the government will prevail.

Cross-references

For more complete discussions of searches and seizures, *see generally Privacy Law and the USA PATRIOT Act,* Chapters 2 and 4.

For more complete discussions of the Foreign Intelligence Surveillance Act of 1978 (FISA) in various

contexts, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 1, 2, 4, 7, 9, 10, and 12.

For more complete discussions of the NSA domestic surveillance program(s), *see Privacy Law and the USA PATRIOT Act, §§ 4.37*--4.47.

For more complete discussions of terrorist designations in various contexts, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 3, 4, 5, 6, and 8.

For more complete discussions of the state secrets privilege, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 2, 4, 6, and 9.

http://www.lexis.com/research/xlink?&source=300346&searchtype=boolean&target=toc

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

Posner on Arar v. Ashcroft

2008 Emerging Issues 1447

Posner on Arar v. Ashcroft

By Steve C. Posner

December 11, 2007

SUMMARY: Is it true that victims of "extraordinary rendition," people who allege they have been shipped by the United States government to other countries to be tortured, have no recourse in United States courts? Does the state secrets privilege always foreclose their claims? What possibly viable claims have not been raised in recent cases? Find out what can be learned from Arar v. Ashcroft.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: Of recent concern is the United States governments practice of extraordinary rendition, the capture and transfer of a person from one nation to another for legal or political purposes. A typical early use of extraordinary rendition is found in *Alvarez-Machain v. United States, 331 F.3d 604 (9th Cir. 2003)*. In *Alvarez-Machain*, Mexican citizens acting for the United States Drug Enforcement Agency (DEA) kidnapped a Mexican national who was then brought to the United States to stand trial. n1

But it is the opposite type of extraordinary rendition that has become the focus of public concern: Detaining a person on United States soil and transferring that person to a foreign nation to be tortured for information in ways that would be illegal if done inside the United States. The two best-known cases of this type are *El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007), cert. denied 128 S.Ct. 373, 169 L.Ed.2d 258 (2007),* and *Arar v. Ashcroft, 414 F. Supp. 2d 250 (E.D. N.Y. 2006)*. While *El-Masri* simply dismissed the complaint on the ground that the action could not be litigated without threatening the disclosure of state secrets, *Arar* is more instructive because the court analyzed the statutory bases of Arars four claims, affirming the dismissal of three on the merits, and holding the state secrets privilege irrelevant to the fourth claim, which was allowed to proceed.

According to the complaint, Arar is a Syrian native who became a dual citizen of Canada and Syria, living in Canada. He returned from a Tunisian vacation through Switzerland and then through John F. Kennedy Airport in New York, where he was found to be on a terrorist watch list as a suspected member of Al Qaeda. He was detained, interrogated, placed in solitary confinement, and denied a lawyer. He was offered an opportunity to voluntarily return to Syria, but he expressed fear of being tortured there, and asked to be sent to Canada or back to Switzerland. He was asked to sign a form that he was not allowed to read, and was then transferred to a Brooklyn detention center, where he was kept in solitary confinement and, again, denied a lawyer. The Immigration and Naturalization Service initiated removal proceedings. Allowed one telephone call, he contacted his family, who contacted the Canadian Consulate and

retained counsel. A Canadian Consulate official visited Arar and assured him that he would not be removed to Syria. His lawyer visited him, but the following day, INS officials interrogated him without giving notice to his lawyer. The INS determined that Arar was a member of Al Qaeda and ordered that he be removed to Syria. He was loaded into a small jet, flown to Jordan, and handed over to the Syrians, who tortured him for ten months before releasing him to Canadian Embassy officials in Damascus. He was then flown home to Canada and reunited with his family.

Arar sued United States officials in their official capacities for violation of the Torture Victim Prevention Act by conspiring with Jordanian and Syrian officials to bring about his torture; violating his Fifth Amendment substantive due process rights by knowingly and intentionally subjecting him to torture and coercive interrogation in Syria; arbitrary and indefinite detention in Syria (also in violation of his Fifth Amendment substantive due process rights); and subjecting him to outrageous conditions of confinement and coercive interrogation in the United States while being denied access to lawyers and the courts.

The trial court dismissed the Torture Victim Prevention Act claim on the ground that individuals are liable only for torture committed under actual or apparent authority, or color of law, of any foreign nation. Since the named defendants had acted under color of United States law, not foreign law (despite the actions of the Jordanian and Syrian officials, who acted under color of their own law), the TVPA claim could not stand. Had Syrian officials ordered United States officials to torture Arar, the United States officials might have been deemed to have acted under color of foreign law, but as things stood, dismissal was required.

The trial court, in *dicta*, found highly relevant the Foreign Affairs Reform and Restructuring Act of 1998 (FARRA), *105 P.L. 277*, Div. g., Title XXII, § 2242, *112 Stat. 2681-922* (Oct. 21, 1998) (codified as Note to *8 U.S.C. § 1231*), because the regulations derived from it, *8 C.F.R. §§ 208.16--208.18*, prohibit sending individuals to countries where they are more likely than not to be tortured. But there is no private right of action under FARRA, and so, the court noted, Arar made no claim under it. *See Arar, supra at 266*, 263--264.

The court gave no credence to defense arguments that it lacked subject matter jurisdiction to review Arars Fifth Amendment substantive due process claims regarding his overseas detention and torture. However, it dismissed the claims. Declining to resolve whether the Fifth Amendment provided Arar with substantive due process protection, the court found his claims foreclosed under an exception to *Bivens v. Six Unknown Narcotics Agents, 403 U.S. 388, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971)*--the existence of special factors counseling hesitation. *Chappell v. Wallace, 462 U.S. 296, 298, 103 S.Ct. 2362, 2365, 76 L.Ed.2d 586 (1983)*. The special factor that persuaded the court was that [the] national-security concerns raised here are properly left to the political branches of government. *Arar, supra at 281*. The court observed that the regulation of aliens is placed with Congress by Article I, Section 8 of the United States Constitution; that Congress had not taken a position on extraordinary renditions; that it had declined to provide a private cause of action to plaintiffs like Arar under the TVPA, or to any plaintiff under FARRA; and that there are crucial national-security and foreign policy considerations at issue. *See id. at 281*--283. Moreover,

[T]here is a fundamental difference between courts evaluating the legitimacy of actions taken in the domestic arena and evaluating the same conduct when taken in the international realm [J]udges have neither the experience nor the background to adequately and competently define and adjudge the rights of an individual vis--vis the needs of officials acting to defend the sovereign interests of the United States. [A] judge who declares on his or her own Article III authority that the policy of extraordinary rendition is under all circumstances unconstitutional must acknowledge that such a ruling can have the most serious of consequences to our foreign relations or national security or both. Without explicit legislation, judges should be hesitant to fill an arena that, until now, has been left untouched perhaps deliberately--by the Legislative and Executive branches. To do otherwise would threaten our customary policy of deference to the President in matters of foreign affairs. (Citations omitted.)

Id. at 282--283.

The court allowed Arar to proceed with his challenge to his thirteen-day period of detention within the United

States, but required Arar to re-plead his case to allege with adequate detail which defendants directed, ordered and/or supervised the violations of his due process rights. The court found no merit to the defense that aliens detained at the border have no substantive due process rights. Nor did the court find that the defendants were protected by qualified immunity.

The court did not address the state secrets privilege regarding Counts 1 thru 3, finding the doctrine moot, and noted that the government had not raised the privilege with regard to Arars detention inside the United States.

Additional Analysis. The practitioner contemplating an extraordinary rendition case should note a significant distinction between *Alvarez-Machain* and *Arar*. In *Alvarez-Machain*, plaintiff raised a claim under the Federal Tort Claims Act. The Ninth Circuit noted that, although the FTCA bars suit for any claim arising in a foreign country (*28 U.S.C. § 2680(k)*), a claim can still proceed under the headquarters doctrine if harm occurring in a foreign country was proximately caused by acts in the United States. *Alvarez-Machain at 638, citing Nurse v. United States, 226 F.3d 996, 1003 (9th Cir. 2003)* and *Cominotto v. United States, 802 F.2d 1127, 1130 (9th Cir. 1986)*. The court observed that [t]he quintessential headquarters claim involves federal employees working from offices in the United States to guide and supervise actions in other countries.

In *Arar*, no FTCA claim was raised but such a claim regarding Arars overseas torture might have survived on the merits, although the claims actually alleged failed.

The practitioner should consider an FTCA claim because *28 U.S.C. § 2679* provides that the FTCA (*28 U.S.C. §§ 2671--2680*) is the exclusive remedy for a claim of damages arising from any negligent or wrongful act or omission of any employee of the Government while acting within the scope of his office or employment. § 2679(b)(1). The coverage of this statute is broad; courts have found even vicious conduct to be within the scope of employment. *See Valerie Plame Wilson v. I. Lewis Libby, Jr., 498 F. Supp. 2d 74, 98 (D. D.C. 2007)* (The alleged means by which defendants chose to rebut Mr. Wilsons comments and attach his credibility may have been highly unsavory. But there can be no serious dispute that the act of rebutting public criticismby speaking to members of the press is within the scope of defendants duties as high-level Executive Branch officials.)

Attorneys contemplating an FTCA claim should take care, however, that their plaintiff has exhausted his administrative remedies. *See 28 U.S.C. §§ 2679*(d), 2675(a); *Wilson, 498 F. Supp. 2d at 99*.

Nor did *Arar* raise the common law claims set forth in *Alvarez-Machain*. In *Alvarez-Machain*, a common law false arrest claim against United States officials was sustained with regard to the plaintiffs overseas kidnapping. Similar common law abuse claims might survive for overseas torture.

Conclusion. The above-cited statutes and cases can help counsel prepare claims in extraordinary rendition cases.

Cross-references.

For further discussion of extraordinary rendition, *see Privacy Law and the USA PATRIOT Act, § 6.09.*

For further discussion of searches and seizures, *see Privacy Law and the USA PATRIOT Act, Chapters 2* and 4.

For further discussion of the Foreign Intelligence Surveillance Act of 1978 (FISA) in various contexts, *see Privacy Law and the USA PATRIOT Act, Chapters 1*, 2, 4, 7, 9, and 10.

For further discussion of the NSA domestic surveillance program(s), *see Privacy Law and the USA PATRIOT Act, §§ 4.37*--4.47.

For further discussion of terrorist designations in various contexts, *see Privacy Law and the USA PATRIOT*

Act, Chapters 3, 4, 5, 6, and 8.

For further discussion of the state secrets privilege, *see Privacy Law and the USA PATRIOT Act, Chapters 2*, 4, 6, and 9.

Return to Text

n1 . After the United States Supreme Court held that a court had power to try even a kidnapped defendant, Alvarez-Machain stood trial, was acquitted, and then sued his Mexican kidnappers, certain DEA agents, and the United States for kidnapping; torture; cruel, inhuman, and degrading treatment or punishment; arbitrary detention; assault and battery; false imprisonment; intentional infliction of emotional distress; false arrest; negligent employment; negligent infliction of emotional distress; and constitutional torts under the Fourth, Fifth and Eighth Amendments to the United States Constitution. Statutory claims were brought under the Federal Tort Claims Act, *28 U.S.C. §§ 1346(b)(1), 2671-2680*; the Alien Tort Claims Act, *28 U.S.C. § 1350*; and the Torture Victims Prevention Act of 1991 (TVPA), *102 P.L. 256, 106 Stat. 73.* The trial court allowed recovery under the Alien Tort Claims Act and the Federal Tort Claims Act (FTCA) for his detention in Mexico. Recognizing that Congress had not statutorily granted the DEA unlimited enforcement powers abroad, the Ninth Circuit held that Alvarez-Machain had established a tort committed in violation of the law of nations. The Ninth Circuit also reversed the trial courts dismissal of the false arrest claim.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

8 of 12 DOCUMENTS

Posner on Al-Haramain Islamic Found., Inc. v. Bush

2008 Emerging Issues 1424

Posner on Al-Haramain Islamic Found., Inc. v. Bush

By Steve C. Posner

December 11, 2007

SUMMARY: As the war on terror moves the nation into uncharted legal territory, Al-Haramain raises important and fascinating issues: How is the state secrets privilege to be analyzed, and what are its outer boundaries? If the government inadvertently discloses a state secret, can a litigant use it in evidence? Does the Foreign Intelligence Surveillance Act pre-empt the state secrets privilege?

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ARTICLE: *Al-Haramain Islamic Found., Inc. v. Bush, 2007 U.S. App. LEXIS 26568 (9th Cir., Nov. 16, 2007)*, is the latest in a recent spate of cases in which the federal government has asserted the "state secrets" privilege-a common law evidentiary privilege that allows the government to deny discovery of military secrets. Assertion of this privilege, if upheld by the courts, can deny a plaintiff legal recourse for government abuses in two ways:

1. If the very subject matter of the suit is a state secret, the suit must be dismissed without reaching any questions of evidence. The case is non-justiciable in a way similar to a political question.

2. Denial of discovery may prevent the plaintiff from being able to prove either standing or a *prima facie* case, thus, requiring dismissal.

At least one court, the Fourth Circuit, has merged these two analytical steps into one. *See El-Masri v. United States, 479 F.3d 296, 302 (4th Cir. 2007)* (broadly equating the subject matter of a suit with the ability to prove a *prima facie* case). However, in *Al-Haramain*, the Ninth Circuit, like the District of Columbia Circuit, n1 rejected the Fourth Circuit's analysis and held that the fact that a case involves privileged information does not render the very subject matter of the action a state secret. *See Al-Haramain* at *28-30. Thus, a split of authorities has been created between the Fourth and the Ninth/D.C. Circuits.

Al-Haramain is particularly interesting because it involved both allegations that the National Security Agency ("NSA") violated the Foreign Intelligence Surveillance Act ("FISA") in conducting warrantless domestic electronic surveillance, and a claim by the plaintiff, an Islamic foundation (the "Foundation") that it had evidence that it was a warrantless surveillance target. This gave the Foundation a clearer claim to standing than in any of the other recent state secrets cases, although the claim to standing ultimately failed on appeal. *Al-Haramain* is also interesting because it

collected and summarized publicly available information about the NSA's domestic electronic surveillance program. n2 Finally, it raised, but did not resolve, the question of whether FISA pre-empts the state secrets privilege.

The evidence was in the form of a document that the government inadvertently gave to the Foundation in 2004 during a proceeding to freeze the Foundation's assets, which apparently stated that the Foundation had been a target of the Terrorist Surveillance Program ("TSP"), the name given by the government to the publicly-acknowledged NSA surveillance program. After the inadvertent disclosure, the document, which was labeled "TOP SECRET," was disseminated by the Foundation's counsel to the Foundation's directors and to co-counsel, and was reviewed by a *Washington Post* reporter. Subsequently, the FBI retrieved all copies of the document from the Foundation's lawyers, although not from its directors.

Although the government has acknowledged the program, it has not disclosed the identities of the program's targets.

The Foundation sued the government for violating the United States Constitution (Amendments IV, V and VI), FISA, and the International Covenant on Civil and Political Rights. The Foundation offered a sealed copy of the document as evidence.

The government moved to dismiss, asserting that the very subject matter of the action was a state secret. The government also asserted that the document was privileged and inadmissible.

The trial court denied the government's motion, finding that the existence of the TSP was not a state secret, and that "no harm to the national security would occur if plaintiffs are able to prove the general point that they were subject to surveillance as revealed in the Sealed Document, without publicly disclosing any other information contained in the Sealed Document." *Al-Haramain Islamic Foundation, Inc. v. Bush, 451 F. Supp. 2d 1215, 1224 (D. Or. 2006)*. The trial court granted the government's motion to bar the Foundation from access to the document but permitted witnesses to file *in camera* affidavits attesting from memory to the document's contents to support the Foundation's assertions of standing and its *prima facie* case. But the trial court also certified its order for interlocutory appeal.

The Ninth Circuit reviewed the trial court's determination of law *de novo.* It agreed with the trial court that the subject matter of the case was not a state secret, because the government had publicly disclosed the TSP and because the Foundation had been publicly designated a terrorist organization.

However, the Ninth Circuit held that two evidentiary items were subject to the state secrets privilege, even though the plaintiffs were fully aware of them because the government had disclosed them: (1) evidence that the Foundation had been a TSP target; and (2) the physical document.

Since the physical document was privileged, it was unavailable as evidence, "as though a witness had died" *(2007 U.S. App. LEXIS 26568* at *37). The Ninth Circuit also reversed the trial court and refused to allow witnesses to testify to the contents of the document from memory because, it held, this would violate the document's absolute privilege. Thus, it ruled, the Foundation could not establish standing and the case would have to be dismissed. However, since it is possible that FISA's "aggrieved person" procedures (*see 50 U.S.C. § 1806)* pre-empt the state secrets privilege, the Ninth Circuit remanded the case to the trial court for determination of this question.

Additional Analysis. Such cases as *El-Masri* and *Al-Haramain* venture into poorly mapped legal territory, in which all possible routes to a desired legal conclusion must be considered. In *Al-Haramain*, plaintiffs have done just that by raising *50 U.S.C. § 1806(e)*. This statute allows an "aggrieved person," that is, a person against whom electronic surveillance evidence has been used or disclosed in any proceeding before "any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof" to move to suppress the evidence if the evidence was not legally acquired or "the surveillance was not made in conformity with an order of authorization or approval." Under § 1806(f), the court must then determine whether the surveillance was legally conducted. If the court determines that the surveillance was conducted illegally, then the person who conducted it is

subject to up to five years imprisonment and a fine of up to $10,000.00 (*see 50 U.S.C. § 1809),* as well as a civil liability amounting to the greater of $1,000.00 or $100 per day, plus punitive damages, plus reasonable attorney fees and costs (*see 50 U.S.C. § 1810).*

A key question is whether the government's act in designating an individual or organization as terrorist, or in freezing assets, is a "proceeding." *Al-Haramain* expressly describes "a proceeding to freeze the organization's assets." *Id*. at *3. The case also describes "Al-Haramain's civil designation proceeding." *Id*. at *8. Therefore, both asset freezing and terrorist designation are arguably "proceedings" subject to the FISA "aggrieved person" statutes.

Al-Haramain also raises the possibility that FISA § 1806 can be applied to terrorist designations, alien removal proceedings, etc. If such proceedings are based on evidence derived from illegal electronic surveillance, § 1806 mandates that the evidence be suppressed, and, if there is nothing else on which the government can ground its proceeding, a designation or removal may be illegal. Moreover, § 1806(e) allows such a challenge in the context of a government decision already made if "there was no opportunity to make such a motion or the person was not aware of the grounds of the motion." This could provide an alternative avenue for challenging designations to the administrative proceeding established in *31 C.F.R. § 501.807,* or the procedures for challenging removal orders under immigration law.

Since *50 U.S.C. § 1806(a)* provides that "[n]o otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this *title [50 USCS §§ 1801* et seq.] shall lose its privileged character," an important question is whether an aggrieved person must have evidence that illegal electronic surveillance occurred or minimization procedures were not followed before moving to suppress the evidence. *50 U.S.C. § 1806(e)* does not seem to require that the aggrieved person possess actual knowledge or evidence that electronic surveillance evidence was used; it appears to be enough that "evidence obtained or derived from an electronic surveillance..has been, introduced or otherwise used or disclosed" in a government proceeding.

Conclusion. The war on terror continues to give rise to prismatic cases in which constitutional and statutory privacy rights, terrorist designations, electronic surveillance statutes, criminal law, and the state secrets privilege are key facets. Even though government power has increased since the events of 9/11, the interplay among these facets gives rise to new arguments attorneys can use to defend clients.

Cross-references

For further discussions of searches and seizures, *see* generally *Privacy Law and the USA PATRIOT Act, Chapters 2* and 4.

For further discussions of the Foreign Intelligence Surveillance Act of 1978 ("FISA") in various contexts, *see* generally, *Privacy Law and the USA PATRIOT Act, Chapters 1*, 2, 4, 7, 9, 10.

For further discussions of the NSA domestic surveillance program(s), *see Privacy Law and the USA PATRIOT Act, §§ 4.37,* et seq.

For further discussions of terrorist designations in various contexts, *see* generally, *Privacy Law and the USA PATRIOT Act, Chapters 3*, 4, 5, 6, and 8.

For further discussions of the state secrets privilege, *see* generally, *Privacy Law and the USA PATRIOT Act, Chapters 2*, 4, 6, and 9.

Return to Text

n1 . *In re: Sealed Case, 494 F.3d 139 (D.C. Cir. 2007)* (holding that Plaintiff had enough evidence independent of state secrets privileged information to make out a *prima facie* case).

n2

[2]. The most significant information for those concerned about the scope of the program came from a speech by General Michael V. Hayden to the National Press Club on January 23, 2006, stating that:

1. At least one participant in each surveilled call was located outside the United States;

2. The surveillance was conducted without FISA warrants;

3. Inadvertent calls involving purely domestic callers were destroyed and not reported;

4. The inadvertent collection was recorded and reported; and

5. U.S. identities are expunged from NSA records of surveilled calls if deemed non-essential to an understanding of the intelligence value of a report.

PDF LINK: Click here for enhanced PDF of this Emerging Issues Analysis at no additional charge

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

Posner on The Obtain/Use Surveillance Dichotomy

2008 Emerging Issues 889

Posner on The Obtain/Use Surveillance Dichotomy

By Steve C. Posner

November 7, 2007

SUMMARY: Much attention has recently been paid to expanded government powers to obtain information about people, but there has been less focus on how such information can be used in prosecutions. The Protect America Act of 2007 has expanded the governments power to conduct warrantless surveillance under the Foreign Intelligence Surveillance Act without individualized targeting of such surveillance, where targets are reasonably believed to be located outside of the United States. A related commentary on Mayfield v. United States explores new grounds for opposing the introduction of FISA evidence into criminal prosecutions.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Although the Fourth Amendment to the United States Constitution is part of the bedrock of American law, its protections have eroded in recent years. One reason is that the Fourth Amendment protects only against unreasonable searches and seizures. At least as far back as *United States v. Miller, 425 U.S. 435 (1976),* the Supreme Court held that congressional action can determine when a persons expectation of privacy is reasonable. Thus, in *Miller*, the Court held that the Bank Secrecy Act of 1970s mandate that banks keep information concerning individuals, implied that individuals have no reasonable expectation of privacy in their bank records. Although the Constitution is superior to statute, as a practical matter statute more often limits the Fourth Amendment than the other way around. Since *Miller*, we have seen a plethora of statutes in which Congress determines when an expectation of privacy is reasonable. This is especially true of surveillance laws such as the Electronic Communications Privacy Act, the Stored Communications Act, the pen register/trap and trace statutes, and, most recently, the Foreign Intelligence Surveillance Act, as amended by The Protect America Act. The recent case of *Mayfield v. United States of America, 2007 U.S. Dist LEXIS 72071 (D. Ore. 2007), summarized the fluctuating situation:*

Now, for the first time in our Nations history, the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes.

The Protect America Act of 2006, and the *Mayfield* case, starkly illustrate two related areas of concern in the surveillance/prosecution process: First--and most widely discussed--how the government obtains information about people. Second--and less discussed although equally of concern--how the government uses the information it obtains. This commentary addresses the Protect America Act, which expands government power to obtain information. For

limits on use in criminal proceedings, please see the commentary on *Mayfield***.**

Responding to concerns about the legality of the National Security Agencys domestic warrantless surveillance program, Congress passed The Protect America Act, Public Law No. 110-55, signed into law by President George W. Bush on August 5, 2007. The Act amended the Foreign Intelligence Surveillance Act (FISA) of 1978, and became effective immediately. It had several effects that, given the Acts 180-day expiration date, may or may not prove permanent:

(1) It excludes from the definition of electronic surveillance any surveillance directed at a person reasonably believed to be located outside of the United States. Thereafter, the Act calls a surveillance an acquisition. *50 U.S.C. §1805A*. (For claritys sake, this commentary will continue to call it surveillance.)

(2) It allows the Director of National Intelligence (DNI) and the Attorney General (AG), to authorize surveillance for up to one year of persons reasonably believed to be located outside the United States, provided that:

a. there are procedures approved by the Foreign FISC for determining that the surveillance concerns persons reasonably believed to be located outside the United States. *See 50 U.S.C. § 1805B*(a)(1);

b. the surveillance does not constitute electronic surveillance as defined in *50 U.S.C. § 1801(f). See 50 U.S.C. § 1805B*(a)(2);

c. the foreign intelligence information is acquired from or with the assistance of a communications service provider. *See 50 U.S.C. § 1805B(a)(3)*;

d. a significant purpose of the acquisition is to obtain foreign intelligence information. *See 50 U.S.C. § 1805B*(a)(4); and

e. FISA minimization procedures are complied with, as defined in *50 U.S.C. § 1801(h). See 50 U.S.C. § 1805B*(a)(5).

The determination must be reduced to a written certification within 72 hours of being made and must be transmitted under seal to the FISC as soon as practicable.

(3) It eliminates the requirement that the government describe with particularity specific facilities, places, premises, or properties at which search or seizure will occur.

(4) It gives the DNI and AG authority to direct a person to immediately provide the government with all information, facilities and assistance needed to accomplish the surveillance secretly and with minimum interference with services provided to the target of the surveillance; and to maintain under DNI and AG-approved security procedures any records concerning the surveillance that the person providing the assistance wishes to maintain. The government can ask the FISC for an order compelling compliance on penalty of contempt. Although a directive can be challenged in the FISA Court, a judge can grant relief only if the directive does not meet the requirements of the new law or is otherwise unlawful. The government must pay for the assistance it receives at the prevailing rate.

(5) It provides a safe harbor for any person who provides information, facilities, or assistance in accordance with a directive.

The Act eliminates any need for individualized suspicion regarding persons covered by it. In order to be exempt from the definition of electronic surveillance, a surveillance need only be directed at a person or persons reasonably believed to be located outside the United States. It is unclear whether a *specific* person or persons must be targeted, although that is implied by the statement that a certificationis not required to identify the specific facilities, places, premises or property at which the acquisition of foreign intelligence information will be directed. *50 U.S.C. § 1805B(b)*.

Even if a specific person or persons must be targeted, however, no individualized suspicion that the target plays one of the roles identified in *50 U.S.C. § 1801(a)* is required. There must merely be a determination and certification that a significant purpose of the surveillance is to obtain foreign intelligence information.

The Act is also vague as to *when* a target is considered to be located outside the United States. As used in the definitional section of FISA, location seems to be determined at the time a communication is intercepted. *See 50 U.S.C. § 1801*(f)(3). This leads to questions. Under a law authorizing year-long surveillance, *when* must a person be located outside the United States? At the moment the DNI and AG make their determination? What if the target is a United States citizen who travels to Canada for one day; can the government surveil him for the next 364 days even if he is in the United States for that entire time?

The phrase reasonably believed also raises questions. If the government reasonably but wrongly believes--because, for example, of misidentification--that a target is outside the United States at the moment of determination, can the government continue to surveil the misidentified United States citizen who has never left the country? As stated by the Congressional Research Service Report on the Act:

Because section 105B [codified as *50 U.S.C. § 1805B*] does not specify where such acquisitions may occur or from whom, it appears that such foreign intelligence information concerning persons reasonably believed to be outside the United States may be acquired, at least in part, from persons, including U.S. persons, who are located within the United States.

Elizabeth B. Bazan, Congressional Research Service, P.L. 110-55, the Protect America Act of 2007: Modifications to the Foreign Intelligence Surveillance Act, (Aug. 23, 2007), Order Code RL34143, at p. 11.

The Protect America Acts expansion of FISA information-*gathering* powers raises important questions regarding the *use* of such information in criminal proceedings.

Evidence gathered under FISA can be kept and introduced in a criminal trial. *See 50 U.S.C. § 1801*(h)(3); *United States v. Falvey, 540 F. Supp. 1306 (E.D. N.Y. 1982).* It has recently been held that such evidence can be kept and used even after the related foreign intelligence investigation has terminated. *See United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2006).* These questions have taken on increased importance since passage of the USA PATRIOT Act (Public Law 107-56, Oct. 26, 2001), because FISA surveillance has, for the past five years, been permitted even if conducted primarily for a criminal investigation purpose, as long as some significant foreign intelligence purpose exists. *See* PATRIOT Act § 218 *codified at 50 U.S.C. §§ 1804*(a)(7)(B) and 1823(a)(7)(B); *In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intell. Surveil Ct. Rev. 2002).*

Courts have also held that the Fourth Amendment exclusionary rule does not apply to FISA evidence because courts apply a foreign intelligence exception to the rule. *See, e.g. United States v. Marzook, 435 F. Supp. 2d 778 (N.D. Ill. 2006),* leaving as a defendants only recourse a motion to suppress under *50 U.S.C. § 1806(e).* Because The Protect America Act is only a year old, and since, in any event, all petitions for review of a government directive are to be filed under seal with the Foreign Intelligence Surveillance Court of Review, and, upon government request, reviewed *ex parte* and *in camera*, publicly available precedents interpreting the Act have been few. The most significant related case is *Mayfield, supra*, holding unconstitutional USA PATRIOT Act § 218, which amended *50 U.S.C. §§ 1804* and *1823* to allow FISA searches in investigations that are not primarily for foreign intelligence purposes.

Conclusion. The Protect America Act of 2007 grants unprecedented and vaguely defined discretion to the Director of National Intelligence and the Attorney General to conduct surveillance of the electronic communications of persons determined to be located outside of the United States, under conditions that will make it difficult to challenge the admissibility of such evidence in criminal trials. It also creates a term of art, acquisition, that, though now legally distinct from electronic surveillance, is an electronic surveillance in all but name. The Protect America Act is currently under review by Congress.

Cross-references

For more complete discussions of the Foreign Intelligence Surveillance Act of 1978 (FISA) in various contexts, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 1, 2, 4, 7, 9, 10, and 12.

For a more complete discussion of *United States v. Miller, 425 U.S. 435 (1976)*, *see Privacy Law and the USA PATRIOT Act, § 5.01*[1].

For a more complete discussion of surveillance statutes and of the distinctions between Title III and FISA in the application of various surveillance technologies, *see Privacy Law and the USA PATRIOT Act, § 2.07*--2.14 and Chapter 4.

For more complete discussions of the amendments to Title III and FISA by the USA PATRIOT Act and other recent statutes, and their effects, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 4 and 7.

For a more complete discussion of the significant purpose rule, the fall of the wall between foreign intelligence and criminal investigation, and its effect on the evidentiary use of FISA evidence, *see Privacy Law and the USA PATRIOT Act, § 2.07*--2.14, 4.30, 4.36--4.47, 7.03.

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

10 of 12 DOCUMENTS

Posner on Mayfield v. United States of America

2008 Emerging Issues 890

Posner on Mayfield v. United States of America

By Steve C. Posner

November 7, 2007

SUMMARY: Much attention has recently been paid to expanded government powers to obtain information about people, but there has been less focus on how such information can be used in prosecutions. Mayfield v. United States purports to limit the governments power to introduce such evidence in criminal trials, and provides defense lawyers with new grounds on which to challenge such evidence. A related commentary on the Protect America Act of 2007 addresses the recent expansion of government powers to conduct warrantless non-individualized basket surveillance.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Since enactment of the USA PATRIOT Act (Public Law 107-56, 2001), the expansion of FISA information-*gathering* powers raises important questions regarding the *use* of such information in criminal proceedings.

Evidence gathered under FISA can be kept and introduced in a criminal trial. *See 50 U.S.C. § 1801*(h)(3); *United States v. Falvey, 540 F. Supp. 1306 (E.D. N.Y. 1982).* It has recently been held that such evidence can be kept and used even after the related foreign intelligence investigation has terminated. *See United States v. Ning Wen, 477 F.3d 896, 898 (7th Cir. 2006).* These questions have taken on increased importance since passage of the Protect America Act (Public Law 110- 55, 2007) because FISA surveillance has, for the past five years, been permitted even if conducted primarily for a criminal investigation purpose, as long as some significant foreign intelligence purpose exists. *See* PATRIOT Act § 218 *codified at 50 U.S.C. §§ 1804*(a)(7)(B) and 1823(a)(7)(B); *In re Sealed Case, 310 F.3d 717 (U.S. Foreign Intell. Surveil Ct. Rev. 2002).* And now, under the Protect America Act, non-individually targeted basket surveillance of people reasonably believed to be located outside the United States is permitted. For a discussion of recently expanded government powers to obtain information, please see the commentary on the Protect America Act.

Mayfield v. United States of America, 2007 U.S. Dist LEXIS 72071 (D. Ore. 2007), is significant in that it limits use of the information obtained under expanded FISA laws. Mayfield holds unconstitutional the significant purpose rule created by PATRIOT Act § 218, which amended *50 U.S.C. §§ 1804* and *1823* to allow FISA searches in investigations that are not conducted primarily for foreign intelligence purposes.

Brandon Mayfield, an attorney, was subjected to FISA surveillance after a latent fingerprint erroneously associated him with a terror bombing in Madrid, Spain. After his innocence was established, he sued the government and settled for $2 million, plus the right to challenge *50 U.S.C. §§ 1804* and *1823*. On September 26, 2007, the United States

District Court for the District of Oregon issued a declaratory judgment holding those FISA statutes unconstitutional as to searches not conducted primarily for foreign intelligence purposes, and expressly rejected the reasoning of *In re Sealed Case, supra.* As grounds, the *Mayfield* Court found that:

a. The FISA procedure allows the government to avoid traditional Fourth Amendment oversight used to obtain a surveillance order;

b. It vitiates the requirement that probable cause be shown;

c. It allows the government to retain information collected, and use the collected information in criminal prosecutions without providing meaningful opportunity for the target of the surveillance to challenge its legality;

d. Unlike the Fourth Amendment, FISA requires no notice, ever, to the target of the surveillance, that the surveillance has occurred, unless the target is criminally prosecuted;

e. Unlike the Fourth Amendment, FISA does not require particularity regarding the things to be seized and the place to be searched; and

f. FISA authorizes surveillance for up to 120 days, whereas Fourth Amendment/ Title III surveillance can be conducted for only 30-days.

Criminal defense counsel may consider challenging FISA-derived evidence on each of the grounds set forth by the *Mayfield* court. Moreover, counsel might argue that, according to *Mayfield*, the government must again show that the primary purpose of the FISA surveillance was foreign intelligence, not criminal investigation. It is likely that the government will appeal *Mayfield* to the United States Court of Appeals for the Ninth Circuit. But unless *Mayfield* is reversed by the Ninth Circuit or by the United States Supreme Court, it provides grounds to challenge the admissibility of FISA evidence in criminal prosecutions. Nor should counsel give up on a *Mayfield* challenge if similar challenges fail in other jurisdictions. The government has shown the value of persistence in the face of failure in the more than thirty cell site data surveillance cases that have been handed down in the past few years.

Conclusion. The *Mayfield* decision provides grounds to challenge the use of evidence gathered under the Act in criminal prosecutions, demonstrating that expanded government power to obtain information about people is not necessarily the same as being able to use the information against them.

Cross-references

For more complete discussions of the Foreign Intelligence Surveillance Act of 1978 (FISA) in various contexts, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 1, 2, 4, 7, 9, 10, and 12.

For a more complete discussion of *United States v. Miller, 425 U.S. 435 (1976)*, *see Privacy Law and the USA PATRIOT Act,* § 5.01[1].

For a more complete discussion of surveillance statutes and of the distinctions between Title III and FISA in the application of various surveillance technologies, *see Privacy Law and the USA PATRIOT Act,* § 2.07-2.14 and Chapter 4.

For more complete discussions of the amendments to Title III and FISA by the USA PATRIOT Act and other recent statutes, and their effects, *see generally, Privacy Law and the USA PATRIOT Act,* Chapters 4 and 7.

For a more complete discussion of the significant purpose rule, the fall of the wall between foreign intelligence and criminal investigation, and its effect on the evidentiary use of FISA evidence, *see Privacy Law and*

the USA PATRIOT Act, §§ 2.07-2.14, 4.30, 4.36-4.47, 7.03.

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

Posner on United States v. Holy Land Foundation for Relief and Development

2008 Emerging Issues 891

Posner on United States v. Holy Land Foundation for Relief and Development

By Steve C. Posner

November 7, 2007

SUMMARY: The Holy Land Foundation for Relief and Development (HLF) was one of the largest Muslim charities in America, until the government designated it a terrorist organization, froze HLFs assets, and destroyed it. But prosecuting HLF and its officers required the government to meet a different standard, and the government failed. Learn why, and what lessons can be drawn by lawyers who defend designees.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Prior to enactment of the USA PATRIOT Act on October 26, 2001, cases involving material support of terrorism or material support of designated foreign terrorist organizations (FTOs) were rare.

No statute criminalizing the provision of material support or resources to foreign terrorist organizations existed until 1996, when *18 U.S.C. § 2339B* was enacted. n1 Between 1996 and enactment of the PATRIOT Act, eight reported decisions referred to § 2339B. Since Oct. 26, 2001, there have been nearly ninety such reported decisions.

The issues that most typically arise in these decisions are: challenges to the designations of organizations as foreign terrorist; challenges to criminal convictions based on such designations; vagueness challenges to statutory terms; and challenges to sentencing enhancements. These issues are often interrelated.

The Secretary of State has the power to designate an organization as an FTO, pursuant to *8 U.S.C. § 1189(a)(1)*, although differently-titled terrorism designations can be made by various executive branch officials. Challenges to such designations have occasionally been successful, but even successful designation challenges have been futile in appealing § 2339B convictions, because it is the *fact* of designation that is an element of the crime; the *validity* of the designation is irrelevant. n2

Until 2001, the Holy Land Foundation for Relief and Development (HLF) was one of Americas largest Muslim charities. HLFs assets were blocked after it was designated a specially designated terrorist and global terrorist pursuant to Executive Order 13224 in December 2001. HLF filed challenges to the designations, which failed after the courts, noting that a designee does not have the same procedural rights available to criminal defendants at trial, n3 found that:

the administrative record contains ample evidence that (1) HLF has had financial connections to Hamas since its

creation in 1989; (2) HLF leaders have been actively involved in various meetings with Hamas leaders; (3) HLF funds Hamas-controlled charitable organizations; (4) HLF provides financial support to the orphans and families of Hamas martyrs and prisoners; (5) HLF's Jerusalem office acted on behalf of Hamas; and (6) FBI informants reliably reported that HLF funds Hamas. n4

On July 26, 2004, HLF and participating individuals were indicted in the United States District Court for the Northern Division of Texas for violating **§ 2339B**, and specifically, for providing material support to Hamas, which, among other designations, had been designated an FTO in 1997. n5 This support was allegedly in the form of money to charitable organizations that, while not Hamas itself, were operated by or for Hamas.

In its criminal prosecution, the government had to prove that some of this money was routed to the militant arm of Hamas, freed up other funds for use by the militant arm, and was used to spread Hamas ideology and recruit supporters. If the defendants intended that the organizations to whom they gave money should pass the money to Hamas -- as the indictment alleges -- then they violated the clear language of *18 U.S.C. § 2339B*.[6] On the other hand, if the government is unable to prove that the defendants knew the groups to whom they gave money were affiliated with Hamas when they provided support, then the defendants cannot be found guilty under the terms of the statute. n7

Going into trial, the government had a number of evidentiary advantages:

. it had been allowed to search and seize the defendants property without warrants (on the ground that the designation was sufficient to put them on notice that they were subject to search and seizure); n8

. the defense motion for a bill of particulars was denied; n9

. the government was allowed to introduce evidence that defendants relatives were involved with Hamas as circumstantial proof of the allegations that defendants materially supported Hamas; n10

. it was June 4, 2007, about five weeks before the July 16, 2007 trial date, before the trial court ordered the government to provide a full list of organizational recipients of HLF money the government would allege were controlled by Hamas; n11 and

. the government was allowed to introduce evidence from FISA intercepts, to some of which the defense had no access (in part because defense attorneys did not move to have them declassified). n12

(The list above, incidentally, provides an interesting menu of points counsel should consider raising in terrorism, money laundering, RICO, conspiracy, and FISA-related criminal cases.)

Nevertheless, the government was unable to prove its case. On October 22, 2007, after more than a decade of investigations, three years of proceedings, three months of trial and 19 days of deliberations, the jury deadlocked and a mistrial was declared on nearly all counts.

The result highlights the contrast between (1) the court findings, during the designation challenges, that there was ample evidence that the defendants were allied with Hamas; and (2) the criminal court jurys refusal to make similar findings. This may be attributable to the dearth of evidentiary and other procedural rights afforded to challengers of designations. Counsel for designees should consider raising the different outcomes described above during the review of a designation in the hope that a reviewing court will carefully scrutinize the administrative record in providing due process. The result of this case makes such scrutiny especially important, because a failure to convict in criminal court may be of little help to a defendant organization that has already been destroyed by administrative action.

Conclusion. It is unclear whether the government will retry the HLF case. However, whether or not the defendants are ultimately convicted or acquitted, HLF has been shut down by the government and is defunct. This raises the question whether more due process safeguards are needed in court review of government designations. *United States v. Holy Land Foundation for Relief and Development* also provides a useful menu of evidentiary approaches for use in terrorism, money laundering, RICO, conspiracy, and FISA-related criminal cases.

Cross-references

For a more complete discussion of government terrorism designations and their effects, please *see generally Privacy Law and the USA PATRIOT Act*, Chapter 3.

For a more complete discussion of material support of terrorists and foreign terrorist organizations, *see Privacy Law and the USA PATRIOT Act, §§ 8.02* through 8.06.

For more complete discussions of searches and seizures, *see generally Privacy Law and the USA PATRIOT Act*, Chapters 2 and 4.

For more complete discussions of the Foreign Intelligence Surveillance Act of 1978 (FISA) in various contexts, *see generally, Privacy Law and the USA PATRIOT Act*, Chapters 1, 2, 4, 7, 9, 10, and 12.

Return to Text

n1 . *18 U.S.C. § 2339A*, which prohibits providing material support or resources to terrorists, was enacted Sept. 13, 1994, P.L. 103-322, Title XII, § 120005(a), *108 Stat. 2022*, and has been amended several times since then. Sections 2339A and 2339B are closely related in intent, but where § 2339A prohibits material support or resources *by* persons or individuals who know they will be used to commit specified terror crimes, § 2339B prohibits material support *of* designated foreign terrorist organizations, regardless of what that material support is used for. § 2339A is relevant to, but not the focus of, this commentary.

n2 . *United States v. Afshari, 426 F.3d 1150 (9th Cir. 2003).*

n3 . *Holy Land Found. for Relief & Dev. v. Ashcroft, 357 U.S. App. D.C. 35* (Jun. 20, 2003), *cert. denied 158 L. Ed. 2d 153, 124 S. Ct. 1506, 2004 U.S. LEXIS 1656 (2004).*

n4 . *Holy Land Found. for Relief & Dev. v. Ashcroft, 219 F. Supp. 2d 57 (D. D.C. 2002), affirmed 357 U.S. App. D.C. 35* (Jun. 20, 2003), *cert. denied 158 L. Ed. 2d 153, 124 S. Ct. 1506, 2004 U.S. LEXIS 1656 (2004).*

n5 . HLF was also designated by other federal authorities.

n6 . *United States v. Holy Land Found. for Relief & Dev., 2007 U.S. Dist. LEXIS 37464* (N.D. Tx., May 23, 2007).

n7 . *United States v. Holy Land Found., 2007 U.S. Dist. LEXIS 50239* (N.d. Tx., Jul. 11, 2007).

n8 . *United States v. Holy Land Found. for Relief & Dev., 2007 U.S. Dist. LEXIS 32293* (N.D. Tx., May 2, 2007).

n9 . *United States v. Holy Land Found. for Relief & Dev., 2007 U.S. Dist. LEXIS 7675* (N.D. Tx., Feb. 1, 2007).

n10 . *United States v. Holy Land Found. for Relief and Dev., 2006 U.S. Dist. LEXIS 88862* (N.D. Tx., Dec. 8, 2006).

n11 . *United States v. Holy Land Found. for Relief & Dev., 2007 U.S. Dist. LEXIS 40310* (N.D. Tx., Jun. 4, 2007) (Twelve recipient organizations were named in the original indictment).

n12 . *United States v. Holy Land Found. for Relief & Dev., 2007 U.S. Dist. LEXIS 48616* (N.D. Tx., Jul. 5, 2007) (The defense had access, in raw or summarized form, to 77.5% of the intercepts the government intended to use. The defense did not seek declassification of all the FISA intercepts.)

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and

surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.

Posner on United States v. Miller

2008 Emerging Issues 892

Posner on United States v. Miller

By Steve C. Posner

November 7, 2007

SUMMARY: Little known but vastly influential, the U.S. Supreme Courts 1976 decision in United States v. Miller made it the matrix case on individuals constitutional reasonable expectation of privacy in personal records held by third parties. Learn the implications for Congresss power to determine reasonable expectations of privacy in varied contexts, statutory complexities, conflict of law issues at the state and international levels.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Though partly superseded by the Right to Financial Privacy Act of 1978, n1 *United States v. Miller* n2 remains one of the most influential cases n3 on the subject of privacy rights in documents held by third-parties. *Miller* holds that one has no Fourth Amendment reasonable expectation of privacy in ones bank records because [w]hat a person knowingly exposes to the public, is not a subject of Fourth Amendment protection. n4

The holding was based on two premises: (1) Such transactional records are the banks business records, not the property of the person whom those records concern; and (2) Congress has the power to assess what is a reasonable expectation of privacy, and by passing the Bank Secrecy Act, Congress determined that there is no reasonable expectation of privacy in bank records.

The holding has since expanded to the general proposition that an individual has no Fourth Amendment privacy interest in information released to a third party and later conveyed by that third party to a governmental entity. n5

However, a minority of states, California, n6 Colorado n7 and Pennsylvania, n8 hold that their constitutions grant rights greater that those the Fourth Amendment provides. These states dont necessarily require a warrant, and, a subpoena *ducas tecum* may be enough. However, they do require that the individual with whom the subpoenaed records are concerned have an opportunity to challenge the subpoena.

The minority states aside, the general rule in the United States is that of *Miller*. This means that privacy protections for personal records in the hands of third parties exist, if at all, as creatures of statute.

This differs from the law of Europe, in which the privacy of personally identifiable records is of constitutional

dimension, and this difference can put multi-national organizations in an untenable conflict of laws, as happened to the Belgian Swift Consortium when the Department of the Treasury required it to disclose transactional information.

In legislating these protections, Congress has tried to be specific about what reasonable expectations of privacy exist in various contexts, but court jurisdictions vary in their interpretations of Congressional intent. The result has been a welter of different expectations. Thus, the expectation of privacy under the Electronic Communications Privacy Act differs from that under the Stored Communications Act. Whether a person has a greater expectation regarding use of mobile tracking devices to follow her, than regarding the use of her cell phone site data to follow her, varies according to jurisdiction. Required showings of probable cause differ in foreign intelligence investigations from those in criminal investigations, although both can be used in criminal prosecutions. The irony of all this complexity is that it is almost impossible for a reasonable person to know what her reasonable expectation of privacy is on a day to day basis.

Conclusion. The practitioner faced with government introduction of surveilled or subpoenaed evidence must, therefore, carefully discern the constitutional or statutory authority under which the government obtained the information, in order to competently challenge the admission of such evidence.

Cross-references

For more complete discussion of *United States v. Miller* and financial privacy, *see generally Privacy Law and the USA PATRIOT Act,* Chapter 5, *see also* § 2.04[1];

For more complete discussion of the Swift Consortium incident and conflict of laws, *see Privacy Law and the USA PATRIOT Act, § 9.08.*

Return to Text

n1 . *12 U.S.C. §§ 3401 et seq.*

n2 . *425 U.S. 435 (1976).*

n3 . Miller has been cited more than 700 times.

n4 . Citing to *Katz v. United States, 389 U.S. 347, 351 (1967).*

n5 . *United States v. Hambrick, 2000 U.S. App. LEXIS 18665 (4th Cir. 2000).*

n6 . *People v. Lissauer, 169 Cal. App. 3d 413; 215 Cal. Rptr. 335 (Cal. App. 1985).*

n7 . *People v. Mason, 989 P.2d 757 (Colo. 1999).*

n8 . *Commonwealth v. DeJohn, 486 Pa. 32, 403 A.2d 1283, 1291 (Pa. 1979)*

ABOUT THE AUTHOR(S):

Steve C. Posner is the author of the annually updated legal treatise Privacy Law and The USA PATRIOT Act (LexisNexis/Matthew Bender 2006), emphasizing the practical implications, burdens and options for organizations and individuals cooperating with and subject to government evolving reporting requirements, information requests and surveillance.

Mr. Posner frequently speaks on privacy and national security law to professional and community groups, as well as to undergraduate and graduate level university classes.

Mr. Posner is a former editor of the Technology Law and Policy Review column for The Colorado Lawyer magazine, and former co-chair of the Colorado Bar Associations Law and Technology Committee. He is admitted to practice law in Colorado, New York and California, and is in private practice in Evergreen, Colorado.