1 of 19 DOCUMENTS

Do the FISA Procedural Rules Cover the National Security Agency?

2010 Emerging Issues 5025

Carey Lening, Kirsten Koepsel, and Ron Weikers on Whether the National Security Agency is Subject to the Procedural Rules of the Foreign Intelligence Surveillance Act

By Carey Lening, Kirsten Koepsel and Ron Weikers

May 10, 2010

SUMMARY: Years after the Terrorist Surveillance Program and other warrantless surveillance became known publicly, litigation continues and key issues remain unresolved. Practitioners whose clients have been subjects of the government's secret surveillance will here find discussion of one of those issues: Does the Foreign Intelligence Surveillance Act apply to the National Security Agency, which carried out such surveillance?

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

ARTICLE: Although the scope of the National Security Agency's (NSA) monitoring of communications may never be fully known, numerous questions have arisen about the government's use of warrantless intercepts. One important question comes to mind: Is the NSA governed by the procedural rules of the Foreign Intelligence Surveillance Act of 1978 (FISA)? n1

Since 2005, when the Terrorist Surveillance Program (TSP) first made headlines, n2 the federal government has claimed that warrantless wiretaps conducted by the NSA as part of the program are necessary tools against the war on terror and are therefore constitutionally justified. n3 The federal government also challenged critics' cries of extralegal overextension, by citing judicial and congressional support, specifically Congress's passage of the Authorization for Use of Military Force (AUMF). n4

Critics responded that these domestic intercepts at the very least require Foreign Intelligence Surveillance Court (FISC) authorization. n5 The federal government replied that the AUMF supersedes FISA's requirement that the government obtain court approval for an intercept. n6 Regardless what may ultimately be decided by the courts and Congress, one thing is certain: The situation presents a thorny but legally interesting question to practitioners who represent subjects of the government's secret surveillance.

THE ORIGIN AND SCOPE OF FISA.

Prior to passage of FISA, Congress took a relatively hands-off approach toward foreign intelligence surveillance conducted by the executive branch. n7 Although Congress made strides toward limiting or prohibiting most forms of warrantless electronic surveillance with passage of the Omnibus Crime Control and Safe Streets Act of 1968, n8 the

Act placed no limitations on the President's ability to conduct surveillance under the scope of national security. n9

The Watergate scandal raised questions of presidential authority to conduct warrantless surveillance in the interests of "national security," and led in part to the creation of FISA. For the first time, Congress placed affirmative limits on warrantless electronic surveillance. n10 FISA was designed to provide judicial and congressional oversight of the executive's covert surveillance activities, while simultaneously maintaining the secrecy needed to protect national security and preserving individuals' Fourth Amendment guarantees "against unreasonable searches and seizures." n11

Generally speaking, FISA regulates two key forms of surveillance within the United States that may apply to the NSA: electronic surveillance of foreign powers or their agents; n12 and the use of pen registers and trap and trace devices for surveillance in connection with a national-security investigation. n13 Surveillance that does not involve a national-security investigation or the monitoring of a foreign power is therefore outside the scope of FISA. n14 FISA also requires that advance approval be obtained from a specially created federal court, the FISC. n15 The FISC has jurisdiction to grant or deny applications for orders authorizing covered surveillance pursuant to the procedural frameworks of FISA. n16

Before a FISC judge may issue an order, the judge must make specific findings of fact as to whether there is probable cause to believe that the targeted entity is a foreign power or its agent, and, in the case of a U.S. citizen, that the target of the surveillance is not considered an agent of a foreign power solely on the basis of activities protected under the First Amendment, n17 such as mere speech. Although applications are almost invariably granted, n18 a FISC judge has the authority to deny or modify an application. In such cases, the government's statutory remedy is an appeal to the Foreign Intelligence Surveillance Court of Review. n19

FISA also imposes civil and criminal n20 safeguards against unnecessary or unlawful government intrusion. Specifically, § 1810 provides for a private cause of action for an "aggrieved person." n21 An aggrieved person is defined by the statute as "the target of a surveillance or search, or a person whose communications or property was actually subjected to a surveillance or search." n22 Entities that can demonstrate "aggrieved person" status under FISA may recover a minimum of "$100 per day for each day of violation." n23

CASE CHALLENGES.

Since 2005, there have been a number of suits challenging the federal government's use of warrantless wiretaps and searches. n24 Two cases are particularly noteworthy.

In January 2006, the American Civil Liberties Union, along with a number of academics, journalists, and lawyers who regularly communicated with individuals overseas, filed suit against the NSA, claiming that the agency's alleged warrantless monitoring of their telephone and e-mail communications pursuant to the TSP was unconstitutional. n25 On July 6, 2007, the U.S. Court of Appeals for the Sixth Circuit reversed a lower court ruling granting summary judgment in favor of the plaintiffs, and dismissed the entire case. The Sixth Circuit held that the plaintiffs lacked any legal standing to sue as "aggrieved persons" under § 1810, because they could not demonstrate that they had in fact been targets of clandestine surveillance. n26 The court also held that the record did not establish whether the NSA's use of warrantless wiretaps constituted "electronic surveillance" as defined by § 1801(f) of the Act, despite the government's admission that it had intercepted telephone and e-mail communications, because "electronic surveillance" has a very specific and particularized meaning under FISA. n27

In the second case, *Al-Haramain Islamic Foundation, Inc. v. Bush*, n28 a charity operating out of Oregon sued the federal government in 2006, alleging that the plaintiffs (who included two of the charity's attorneys, both U.S. citizens) had been subject to warrantless electronic surveillance. The plaintiffs alleged a variety of constitutional challenges, but also sought recourse under § 1810 of FISA. n29

The government filed a motion to dismiss, asserting that the plaintiffs could not use an inadvertently disclosed classified document in their case and that the common-law state secrets privilege (SSP) required dismissal of the whole

case. n30 Although the district court agreed that the government had properly invoked the privilege, it declined to dismiss the case. Holding that it was necessary to first resolve the question of the plaintiffs' standing to sue, the court first conducted an *in camera* review and allowed the plaintiffs' witnesses to attest from memory as to the contents of the classified document. n31 Shortly thereafter, the trial court certified its order for interlocutory review.

After a lengthy *in camera* review of the classified document, the Ninth Circuit's Court of Appeals determined that the plaintiffs could not establish standing, absent use of the document (then under seal). n32 Declining to address whether FISA preempts the SSP, the appellate court remanded the case to Judge Vaughn R. Walker of the U.S. District Court for the Northern District of California.

Following remand, the government filed additional motions to dismiss, n33 arguing that FISA did not preempt the SSP, and that the SSP presented insurmountable obstacles to the plaintiffs' ability to present their case.

On July 2, 2008, Judge Walker concluded that the legislative history of FISA demonstrated Congress's intent for it to preempt or displace the SSP in cases within its reach. n34 In a separate order issued in January 2009, the court concluded that the plaintiffs had presented enough evidence to demonstrate standing. n35 Finally, on March 31, 2010, the district court determined that the plaintiffs had established a *prima facie* case of warrantless electronic surveillance. n36

ANALYSIS.

Practitioners who represent clients subject to such government surveillance must be mindful of some practical considerations illustrated by these cases. Foremost, standing will remain a perpetual challenge for clients seeking relief under FISA. Like the plaintiffs in *ACLU*, plaintiffs who may have valid Fourth Amendment standing may nonetheless find it difficult to establish a claim as an "aggrieved person" under § 1810. This is particularly true where a nontarget, such as an acquaintance or tenant residing with an agent of a foreign power targeted under an NSA investigation, finds his or her communications also surreptitiously monitored. Although FISA contains a notice provision, notice is required only when the government intends to use "any information obtained or derived from an electronic surveillance of that aggrieved person...." n37

The second practical concern involves the government's application of the SSP to avoid evidentiary disclosure. The plaintiffs in *Al-Haramain* avoided the government's invocation of the privilege and were able to establish their status as targeted individuals under the TSP only after stumbling upon a cache of publicly disclosed information. n38 So long as the government maintains a view that only the government's admission of unlawful electronic surveillance will let plaintiffs satisfy the "aggrieved person" standard under FISA, other litigants wishing to challenge warrantless surveillance by the NSA will be consigned to praying for the assistance of a whistleblower or other serendipity. n39

Return to Text

n1 *50 U.S.C. §§ 1801* to 1812.

n2 The TSP was launched in 2001, shortly after the September 11 attack. Although the specifics of the program have not been fully disclosed, the government acknowledged that the TSP included warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States and the NSA had "a reasonable basis to conclude that one party to the communication is a

member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *at* http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/print/20051219-1.html; s*ee also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

n3 U.S. Department of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), *at* www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf (different version at www.justice.gov/olc/2006/nsa-white-paper.pdf). The government specifically cited Article II, Section 2 of the U.S. Constitution, stating that "The President has the chief responsibility under the Constitution to protect America from attack, and the Constitution gives the President the authority necessary to fulfill that solemn responsibility." *Id*. at 1.

n4 Congress authorized the President to "use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks" in order to prevent "any future acts of international terrorism against the United States." Authorization for Use of Military Force, Pub. L. No. 107-40, § 2(a), *115 Stat. 224 (2001).*

n5 Under *50 U.S.C. § 1804.*

n6 Under § 1804.

n7 Article II, Section 2 vests the President with power as "Commander in Chief of the Army and Navy of the United States," while Article II, Section 3 prescribes that "he shall take Care that the Laws be faithfully executed...."

n8 Pub. L. No. 90-351, *82 Stat. 197,* codified at *18 U.S.C. § 2510* et seq.

n9 To the contrary, the Act explicitly states: "Nothing contained in this chapter ... shall ... affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities ... and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which [such] electronic surveillance... may be conducted." *18 U.S.C. § 2511*(2)(f).

n10 *50 U.S.C. § 1801* et seq.

n11 U.S. Const. amend. IV.

n12 *50 U.S.C. §§ 1801*-1811.

n13 *50 U.S.C. § 1805*(i).

n14 Electronic surveillance of entities not considered to be foreign powers or agents of a foreign power are conducted by the federal government under *18 U.S.C. §§ 2510* to 2522. Surveillance involving pen registers and trap and trace devices outside the scope of a national-security investigation is conducted under *18 U.S.C. §§ 3121* to 3127.

n15 The FISC is composed of eleven federal district judges designated by the Chief Justice of the United States. An appellate court, known as the Foreign Intelligence Surveillance Court of Review, is composed of three district or appellate judges designated by the Chief Justice. *50 U.S.C. § 1803*(a) & (b).

n16 For more information on the specific procedure necessary to obtain FISC court authorization, see *50 U.S.C. §§ 1804*(a) (electronic surveillance), 1842(b)(1) (pen/trap & trace).

n17 *50 U.S.C. § 1805*(a)(2)(A).

n18 From 1979 to 2007, the FISC rejected only nine applications out of a total of 25,358 submitted. Electronic Privacy Information Center, Foreign Intelligence Surveillance Act Orders 1979-2007, *at* http://epic.org/privacy/wiretap/stats/fisa_stats.html. During 2008, the FISC denied just one of 2,082 applications. Letter from Ronald Weich, Assistant Attorney General, U.S. Department of Justice, to The Honorable Harry Reid, Majority Leader, United States Senate 1 (May 14, 2009), *at* http://www.fas.org/irp/agency/doj/fisa/2008rept.pdf.

n19 *50 U.S.C. §§ 1803*(a) & 1822(c).

n20 *50 U.S.C. § 1809* governs the criminal provisions covering unauthorized electronic surveillance. It has yet to be invoked.

n21 *50 U.S.C. § 1810.*

n22 *50 U.S.C. §§ 1810* & 1828. However, foreign powers and agents of foreign powers are explicitly excluded from being "aggrieved persons" under the statute.

n23 *50 U.S.C. § 1810*(a).

n24 *People for the American Way Foundation v. NSA, 462 F. Supp. 2d 21 (D.D.C. 2006); Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), remanded in light of Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 539 F.3d 1157 (9th Cir. 2008); American Civil Liberties Union v. National Security Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006), vacated and remanded, 493 F.3d. 644, 2007 FED App. 0253P (6th Cir. 2007), cert. denied, 552 U.S. 1179 (2008). Hepting* was one of a series of cases challenging telecommunications providers after it was revealed that certain firms, including AT&T Corp., Verizon Communications Inc., and BellSouth Corp., provided the government with the telephone records of tens of millions of U.S. subscribers. In 2008, Congress passed the FISA Amendments Act, Pub. L. No. 110-261 *122 Stat. 2436*, which, among other things, granted wide retroactive and prospective immunity to providers giving such assistance.

n25 Specifically, the plaintiffs alleged that the NSA's use of warrantless wiretapping and data mining violated the First and Fourth Amendments of the Constitution, the separation of powers doctrine, the Administrative Procedure Act, FISA, and other "statutory law." *ACLU, 438 F. Supp. 2d at 758.*

n26 *American Civil Liberties Union v. National Security Agency, 493 F.3d 644, 657, 2007 FED App. 0253P (6th Cir. 2007), cert denied, 552 U.S. 1179 (2008).*

n27 *493 F.3d at 682.* After reciting the various factors involved in defining "electronic surveillance" under *50 U.S.C. § 1801*(f), the Sixth Circuit held that the record offered "no indication as to where the interception may occur or where any surveillance device is located. Nor does it offer any basis to conclude that particular people located in the United States are being targeted."

n28 *451 F. Supp. 2d 1215 (D. Or. 2006), aff'd in part and rev'd in part, remanded, 507 F.3d 1190 (9th Cir. 2007).*

n29 *Id. at 1218.* The plaintiffs also challenged the search on First, Fourth, and Sixth Amendment grounds.

n30 *Id. at 1217.* 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. The document allegedly stated that the Foundation had been, at one time, the target of the TSP. After the initial disclosure, the document was disseminated by the Foundation's counsel to its directors and to co-counsel, and was reviewed by a *Washington Post* reporter.

n31 *Id. at 1224, 1229.* At that time, the court also ordered the plaintiffs to turn over all copies of the classified document.

n32 *Al-Haramain Islamic Foundation, Inc. v. Bush, 507 F.3d 1190, 1206 (9th Cir. 2007).* While the case was on appeal, the Judicial Panel on Multidistrict Litigation transferred it from the District of Oregon to Judge Vaughn R. Walker of the Northern District of California, where it is now part of the multidistrict proceeding in *In re National Security Agency Telecommunications Records Litigation*, MDL Docket No. 06-1791, Case No. C 07-0109 VRW.

n33 *See In re* NSA Telecom Litigation, MDL Docket No. 06-1791, Case No. C 07-0109 VRW, #432/017.

n34 *In re NSA Telecom Litigation, 564 F. Supp. 2d 1109, 1124 (N. D. Cal. 2008).*

n35 *595 F. Supp. 2d at 1085-86.*

n36 *In re NSA Telecommunications Records Litigation, 2010 U.S. Dist. LEXIS 31287,* at *44 (Mar. 31, 2010).

n37 *50 U.S.C. § 1806*(c).

n38 The documents included a number of publicly issued statements by government officials, as well as press coverage disclosing post-9/11 warrantless electronic surveillance activities and a much-publicized hospital room confrontation between then- Attorney General John Ashcroft and then-White House counsel Alberto Gonzales, much of which had surfaced after the initial complaint was filed. *In re* NSA Telecom Litigation, MDL Docket No. 06-1791, Case No. C 07-0109 VRW #458/035 at 5.

n39 *In re* NSA Telecom Litigation, MDL Docket No. 06-1791, Case No. C 07-0109 VRW, #475/049 at 31.

RELATED LINKS: For more complete discussions of the Foreign Intelligence Surveillance Act of 1978 ("FISA") in various contexts, see generally

- Steve C. Posner, 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

- Steve C. Posner, Privacy Law and the USA PATRIOT Act, § 4.37-.47.

For more complete discussions of terrorist designations in various contexts, see generally

- Steve C. Posner, Privacy Law and the USA PATRIOT Act, Chapters 3, 4, 5, 6 and 8.

For more on the state secrets privilege, see generally

- Steve C. Posner, Privacy Law and the USA PATRIOT Act, Chapters 2, 4, 6 and 9;
- Amanda Frost on Government Use of the "State Secrets" Privilege, 2008 Emerging Issues 3062 ;
- Posner on El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007): The State Secrets Doctrine and Extraordinary Rendition, 2008 Emerging Issues 2534.

For more on the Al-Haramain case, see

- Posner on Al-Haramain Islamic Found., Inc. v. Bush, 2008 Emerging Issues 1424.

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

ABOUT THE AUTHOR(S):

Carey Lening is an intellectual property, privacy and technology attorney in Washington, DC. **Kirsten Koepsel** is an intellectual property attorney and works as a Director, Legal Affairs & Tax, Aerospace Industries Association in Arlington, VA. **Ron Weikers** is Managing Partner of Weikers & Co. | Software-Law.com in Manchester, NH, and Adjunct Professor of Law at Franklin Pierce Law Center in Concord, NH. Any views expressed herein are solely the

authors', and do not reflect the views of their respective employers.

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.

2 of 19 DOCUMENTS

2009 Christmas Plot Shows U.S. Failure to Adequately Curtail Terrorist Travel

2010 Emerging Issues 4874

2009 Christmas Plot Shows U.S. Failure to Adequately Curtail Terrorist Travel

By Janice Kephart

February 19, 2010

SUMMARY: Janice Kephart, who was a counsel to the 9/11 Commission, explains how failures to follow recommendations of the Commission led to vulnerabilities the Christmas bomber, Umar Farouk Abdulmutallab, was able to exploit -- and others still could.

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

ARTICLE: Key Facts

Al Qaeda's four plane operations succeeded when four hijacking pilots with four or five support hijackers per plane violently took over four U.S. domestic flights between Boston and Washington D.C. on September 11, 2001. The results were suicide crashes into four U.S. sites, with a total of 2,974 fatalities. Two pilots (one twice) and two hijackers had received immigration secondary screening coming into the United States, for a total of five secondaries, but only one was removed.

Two Al Qaeda plane operations were attempted by individuals in-flight, but failed after the terrorists' clothing carrying the bombs caught fire. The plots were foiled by attentive passengers and crew, not the border or aviation architectures abroad and supported by the United States. These are: (1) the Richard Reid shoe bomb attempt on December 21, 2001, on a flight from Paris to Miami (he had been refused boarding the prior day due to poor behavior in secondary screening) and (2) the December 25, 2009, attempt by Umar Farouk Abdulmutallab. He also received secondary screening at check-in, but it did not result in further scrutiny or a no-board decision.

Introduction

One of the key phrases from the 9/11 Commission report (p. 384; the report is available as its own database on lexis.com) is "for terrorists, travel documents are as important as weapons." The 2009 Christmas Day plot aboard Delta Flight 253 by Umar Farouk Abdulmutallab has made clear to the world that not only are travel documents as important as weapons to terrorists, but executed terrorist plots aimed at the United States on 9/11 and subsequently have incorporated air travel as an essential component. What we have learned about terrorist travel has been significant. Incorporating those lessons learned into an operational architecture has improved border and aviation security significantly, but has yet to edge close enough to ensuring it.

The incredible devastation caused by 9/11 has emboldened Al Qaeda to keep trying. Its leaders know fairly well the loopholes that exist, and will continue to exploit them until they are closed. Interestingly, the installation of strong biometric and watchlist information available at U.S. ports of entry since 9/11, including the "freezing" of identities upon entry through US-VISIT, has propelled Al Qaeda to revert to strategies where plots unfold prior to reaching the United States. Thus, both Richard Reid's December 22, 2001, and Abudulmutallab's December 25, 2009, "explosive fashion" attempts have been on planes originating from Europe and bound for the United States with the plot unfolding in the air prior to reaching a U.S. border checkpoint.

That border security must begin beyond our physical borders was a key lesson learned from 9/11, including the use of intelligence to curb the terrorist travel that can begin with a visa application. That aviation security begins at check-in and continues onboard each and every flight was also a key 9/11 lesson learned.

The loopholes where aviation security meets border security are still wide enough for terrorists to exploit, especially where those loopholes are magnified due to constraints placed upon the United States outside U.S. borders by other nations. Yet these loopholes need not exist. In fact, if the 9/11 Commission recommendations had been fulfilled in both letter and spirit, the Christmas Day Plot of 2009 would never have gotten off the ground, literally or figuratively.

Watchlists, visa adjudication and pre-boarding vetting were all discussed in the *9/11 Final Report* and our staff monograph, *9/11 and Terrorist Travel*. It is from this monograph that the term "terrorist travel" has become a standard, and aviation screening in all its forms -- of identification, watchlist checks, and passenger and cargo screening -- took on heightened importance in the post-9/11 world.

While many new programs and procedures have been put in place, some of the most important 9/11 Commission recommendations in these areas have been ignored because they are complex, were not politically prioritized, or have been indefinitely delayed due to arguments claiming civil liberties violations. The programs and policies that are in place are a tremendous improvement over the pre-9/11 border and aviation screening processes, but without all the recommendations fulfilled, the gaps remain. President Obama has stated more than once that the gaps were huge -- both an inaccurate statement as well as an unfortunate message to send around the world, as it indicates that the U.S. is weak on security. What is accurate is that due to the nature of the plot, the ramifications of these gaps were huge, but not the gaps themselves. It is these small gaps that add up to a huge failure, and a potentially tragic event. Filling these gaps will never 100 percent ensure against another successful terrorist event, but it will edge aviation security closer to that assurance, and it is doable.

The Role of Intelligence

The role of intelligence in preventing terrorist travel is essential, but secondary. At base, what matters the most to stop a plotter such as the 2009 Christmas Day bomber is a robust, dot-connected border and aviation security architecture.

President Obama marked this event as primarily an intelligence failure, and the American media continue to focus on the intelligence failures. Yet from the perspective of a former 9/11 Commission counsel -- whose profession focuses on how terrorists exploit travel and what governments need to do to curb such activity -- President Obama's answer is both too myopic and too politically convenient. The President is myopic because he refuses to see the broader questions of border and aviation security that flow from the Christmas Day suicide bomber's significant breach of both systems. The President's answer is politically convenient because if he acknowledges a weakness in U.S. border security, the chance of the amnesty President Obama has pledged his supporters for nearly 11 million illegal aliens currently in the United States could be defeated when the issue arises for congressional consideration this spring. The majority of Americans have made clear that only if border security is achieved first will the country consider such a massive -- and inevitably insecure -- amnesty.

The Obama administration also has never acknowledged the 9/11 Commission recommendations as a continuing

government goal; instead, it has sought to reverse some key recommendations, including a driver license law known as REAL ID that would better help assure identity security for domestic air travel. Despite making its repeal a legislative priority, the administration failed. Yet in so doing, tightening domestic aviation identity security is significantly delayed. Not an admission any administration would own up to.

Nor has President Obama dealt directly with issues stemming from the government's inability to get up and running a new aviation watchlist, called Secure Flight, which his supporters have opposed for years. Reversing 9/11 Commission recommendations such as these, and ignoring others described in more detail below, have not enabled this President to step back and embrace the Commission's recommendations. Instead, Obama has side-stepped these recommendations with a series of broad statements and narrow fixes aimed at the next Al Qaeda attempt that mimics the Christmas plot, but such narrow fixes may not stop a different type of attack that Al Qaeda tries based on the lessons learned about adjusted U.S. security measures.

Blaming the intelligence community -- something the Obama administration has done more than once -- is simply a convenient hook to hang these failures on, but curing *only* those failures will not provide the efficiency and security the government needs to protect against terrorist travel. To be clear, the role of intelligence in preventing terrorist plots is absolutely essential, but when teamed with border and aviation security, it is relevant only under three circumstances: (1) the intelligence community has prior information on the individual; (2) aviation and border systems have sufficient access to the intelligence in real time; and (3) the decision authority within these systems is sufficient to stop the traveler. If any of these circumstances is lacking and an in-flight terrorist event is planned, the risk of success is high.

9/11 Commission Recommendations

The 9/11 Commission recommendations need to be adhered to and upgraded as we garner more information as to how terrorists and criminals travel. However, many of these recommendations as is, even taken individually, could have been sufficient to stop Abdulmutallab. Here are highlights of recommendations still not in place taken directly from the *9/11 Final Report*, many of which are exactly the failures that have been acknowledged by government officials:

Strategies for Aviation and Transportation Security (p. 390)

Recommendation: Improved use of the "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS [computer assisted airport screening, which applies to checked luggage only] continues. This screening function *should be performed by the TSA* [Transportation Security Administration, created after 9/11], and it should *utilize the larger set of watchlists* maintained by the federal government. [emphasis added] (p. 393)

Recommendation: The TSA and the Congress must give *priority attention to improving the ability of screening checkpoints to detect explosives on passengers*. As a start, each individual selected for special screening should be screened for explosives. [emphasis added] (p. 393)

Terrorist Travel (p. 383)

Recommendation: The United States *should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists*, find terrorist travel facilitators, and constrain terrorist mobility.

Since officials at the borders encounter travelers and their documents first . . . , they must work closely with intelligence officials. [emphasis added] (p. 385)

A Biometric Screening System (p. 385)

When people travel internationally, they usually move through defined channels, or portals. They may seek to acquire a passport. They may apply for a visa. They stop at ticket counters, gates and exit controls at the airports and

seaports. Upon arrival, they pass through inspection points. They may transit to another gate to get on an airplane. . . .

Each of these checkpoints or portals is a screening -- a chance to establish that people are who they say they are and are seeking access for their stated purpose, to intercept identifiable suspects, and to take effective action.

The job of protection is shared among many defined checkpoints. By taking advantage of them all, we need not depend on any one point in the system to do the whole job. The challenge is to see the common problem across agencies and functions and develop a conceptual framework -- an architecture -- for an effective screening system. [emphasis added] (pp. 385-86)

The U.S. Border Screening System

All points in the border system -- from consular offices to immigration services offices -- will need appropriate electronic access to an individual's file. Scattered units at Homeland Security and the State Department perform screening and data mining: instead, a government-wide team of border and transportation officials should be working together. A modern border and immigration system should combine a biometric entry-exit system with accessible files on visitors and immigrants, along with intelligence on indicators of terrorist travel. [emphasis added] (pp. 388-89)

Assessing the 2009 Christmas Plot

In the case of Abdulmutallab, intelligence existed, but there was a gap in aviation and border systems obtaining that information in a timely manner. The intelligence itself was also not sufficiently analyzed or shared across agencies, highlighting issues with inadequate risk-assessment software tools and failures to integrate the border and aviation systems sufficiently with intelligence. It thus was of little consequence that the intelligence was as solid or strong as it was, if it could not reach the right people at the right time with the authority to make the right decisions.

However, had the intelligence and border community had Abdulmutallab's full immigration history available, both a visa revocation and "no fly" instruction would more likely have been generated. A full immigration history should have included the following types of information: (1) the issuance of a two year multi-entry visa at the U.S. Embassy in London in July 2008; (2) use of that visa to visit the United States twice, including Washington D.C. and a religious conference; and (3) intelligence from a CIA station chief located at the U.S. Embassy in Nigeria, who submitted a report to his superiors (but not to the State Department or immigration authorities) cataloguing visits and phone calls from Abdulmutallab's prominent and credible father concerned about his son cutting off communication and his radical leanings in November 2009. (Al Qaeda requires a communication cutoff of families when a sworn member is designated to conduct a mission.) With information shared better with allies, Abdulmutallab's immigration file could also have included notification from the British of a visa denial in May 2009 based on the inclusion of false information on a student visa application.

One fallacy that the U.S. State Department has repeatedly attempted to generate is that it did not have authority to revoke Abdulmutallab's visa. It had more than sufficient authority; statements claiming otherwise are a matter of long-held State Department policy, not legal authority. In fact, the 9/11 Commission recommended and it is law that authority for visa revocations is wide and not challengeable in court. (For example, *8 U.S.C. § 1201(i)*, 8 C.F.R. § 41.122, and related authority cited at the end of this article.) The State Department had enough information and authority to revoke this terrorist's visa, but simply failed to do it. More recently, it claimed that the intelligence community asked the State Department not to revoke Abdulmutallab's visa, yet that fails to jibe with other facts brought out to date. The problem with the visa process is that even since 9/11, it remains an arm of diplomatic favoring and reciprocity around the world. Security is of much lower priority.

On the other hand, U.S. border personnel do conduct intelligence and risk assessments of passenger manifest lists backed up by a security mission, but are hamstrung by both the lack of legal authority to conduct law enforcement activities overseas and a "too small" watchlist vetting process pre-boarding. This is the case even at international airports such as Schiphol in Amsterdam, where the United States has border inspectors on the ground. Yet they were

never tasked with screening Abdulmutallab. Nor would the one inspector on duty at the time Abdulmutallab boarded have had the authority to stop him without agreement from his or her Dutch counterparts, even if the U.S. immigration analysts reviewing his information had requested a secondary screening and no-board order.

Add to that the watchlists being vetted on Christmas Day -- only a narrow "no fly" and "selectee" list were reviewed pre-boarding -- which were wholly inadequate to stop an in-flight terrorist attempt. Had the vetting of more complete watchlists that the 9/11 Commission recommended occurred pre-boarding, a secondary inspection would have been sought. Instead, Abdulmutallab was not scheduled to be questioned by border inspectors until landing in Detroit. The layers were in place, but the timing and content of the layers insufficient.

If the full body scan equipment available at Schiphol had been used, also in tune with 9/11 recommendations, this also could have stopped Abdulmutallab. Another quandary is that TSA personnel are still without direct access to Secure Flight data -- the aviation watchlist tool that has not gone live in eight years due to constant pushback from those claiming civil liberties violations. In addition, integrated intelligence garnered from immigration pre-screening with TSA body scan procedures would inevitably help ensure that a proper architecture is in place to vet the entire person, not just a body, an ID, or a combination of watchlists. Any one of those layers could be sufficient, but this one was not in place. As was said in the *9/11 Final Report*, "the job of protection is shared among many defined checkpoints. By taking advantage of them all, we need not depend on any one point in the system to do the whole job." (p. 386)

There were many opportunities to stop the 2009 Christmas plot, and all fell through gaps because 9/11 Commission recommendations were not fully implemented, even five years after those recommendations were published and most made law. Too little too late is no longer an excuse. Much was in place prior to this administration, and it has been up to President Obama to continue implementation. That President Obama has a second chance is lucky for us all. Let's hope that whether it is by name or not, the 9/11 Commission recommendations become fully implemented. We may not be so lucky next time.

RELATED LINKS: On revocation of visa petitions, see
- 8 U.S.C. 1155;
- Josh Adams, Federal Court Jurisdiction over Visa Revocations, 32 Vt. L. Rev. 291 (2007).

On revoking an immigrant visa, see
- 22 C.F.R. 42.82.

Other information is at
- 6 U.S.C. 236 ;
- 8 U.S.C. 1103.

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

ABOUT THE AUTHOR(S):

Janice Kephart is a former border counsel to the 9/11 Commission and currently serves as National Security Policy Director at the Center for Immigration Studies. Another version of this article appeared in the February 2010 issue of Aviation Security International.

Impact of DHS Private Sector Accreditation Program on Roles and Responsibilities

2010 Emerging Issues 4869

Impact of DHS Private Sector Accreditation Program on Roles and Responsibilities

By Brian Finch

February 17, 2010

SUMMARY: Businesses and other entities wanting to improve preparedness, protect business continuity, or limit potential liability should be aware of the PS-Prep program. DHS is moving to designate standards that are officially voluntary but may well become the measures of due care, as Brian Finch explains.

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

ARTICLE: Introduction

Among the many programs established in the Implementing Recommendations of the 9/11 Commission Act of 2007 (the "9/11 Implementation Act") (Public Law No. 110-53, *121 Stat. 266),* one in particular stands out with respect to its impact on the private sector. Under section 901 (codified at *6 U.S.C. § 321m*), Congress authorized a program designed to create a voluntary system under which private entities could seek accreditation and certification of their preparedness efforts from the Department of Homeland Security ("DHS"). This program, known as the Voluntary Private Sector Preparedness Accreditation and Certification Program ("PS-Prep"), was created with the intent of helping private entities measure their preparedness using objective standards adopted by DHS. Information about PS-Prep is available at http://www.fema.gov/privatesector/preparedness/index.html (last visited Feb. 16, 2010). DHS has announced that it will designate three such standards under PS-Prep, significantly moving the program forward. *74 Federal Register 53,286* (notice Oct. 16, 2009).

Several important questions surround the impact of this program on the private sector, including whether the PS-Prep program is truly voluntary or does in fact raise the standard of care for private entities throughout the United States. A brief examination of the PS-Prep law as well as a critical case in the post-9/11 era reveals that, for many entities, PS-Prep could in fact represent a minimum bar for preparedness against a range of threats, including terrorism.

Background on PS-Prep

PS-Prep, codified at *6 U.S.C. §321l* and 321m, is explicit in its intent and the areas to be covered. As DHS itself stated:

The purpose of the PS-Prep Program is to enhance nationwide resilience in an all-hazards environment by

encouraging private sector preparedness. The program will provide a mechanism by which a private sector entity - a company, facility, not-for-profit corporation, hospital, stadium, university, etc. - may be certified by an accredited third party establishing that the private sector entity conforms to one or more preparedness standards adopted by DHS.

See http://www.fema.gov/media/fact_sheets/vpsp.shtm (last visited Feb. 16, 2010). Noting that there is currently "no comprehensive set of standards by which American businesses and other private sector entities can assess their preparedness for all hazards," DHS has encouraged private entities to consider pursuing certification under one of the standards adopted under PS-Prep.

As set forth in the 9/11 Implementation Act, DHS can develop guidance or recommendations and identify best practices to help or encourage action by the private sector in a range of areas, including:

- identifying potential hazards and assessing risks and impacts;
- mitigating the impact of a wide variety of hazards, including weapons of mass destruction;
- managing necessary emergency preparedness and response resources;
- developing mutual aid agreements;
- developing and maintaining emergency preparedness and response plans and associated operational procedures;
- developing and conducting training and exercises to support and evaluate those plans and procedures;
- developing and conducting training programs for security guards to implement those plans and procedures; and
- developing procedures to respond to requests for information from the media or the public.

6 U.S.C. §321l.

At this time, DHS has announced it will adopt standards from ASIS International (on "Organizational Resilience: Security Preparedness, and Continuity Management Systems"), the British Standards Institution (on business continuity management), and the National Fire Protection Association (on disaster/emergency management and business continuity). DHS describes the standards as "comprehensively" dealing with preparedness and notes that they can be applied to the majority of private entities. DHS has also stated that it might adopt additional standards in the future.

Under the certification process, private entities can then have an accreditation party selected by DHS determine whether they are in compliance with the relevant standard. Here, DHS has selected the ANSI-ASQ National Accreditation Board to develop and oversee the accreditation process, and gave it the authority to accredit third parties to actually carry out the certifications. News Release, Federal Emergency Management Agency, DHS Selects ANSI-ASQ National Accreditation Board To Support Voluntary Private Sector Preparedness Certification Program (July 30, 2008), *available at* www.fema.gov/news/newsrelease.fema?id=45280 (last visited Feb. 16, 2010). Private entities will apply for certification following the process outlined by DHS.

It is important to note here that DHS defines "certification" under the PS-Prep program as "confirmation that an accredited third party certification organization has validated the private sector entity's preparedness to a standard." http://www.fema.gov/media/fact_sheets/vpsp.shtm/. There will be periodic reassessments of the entity so that the certification organization can "continue to have confidence in the organization's conformity to emergency preparedness and business continuity" management systems. Companies that have been certified under PS-Prep are also eligible to have that conformance published on a DHS website. Between the carefully selected standards and the tightly monitored third-party accreditation systems, DHS is looking to fulfill the congressional intent of developing a reliable mechanism to help the private sector raise its preparedness for a wide range of emergency scenarios.

The Impact of PS-Prep on Potential Liability

DHS is careful to state in its PS-Prep documents and processes that the program is completely voluntary. PS-Prep does not create an obligation to go through its process, and there are no consequences for failing to pursue PS-Prep certification.

However, a company's decision as to whether it should go through the PS-Prep process should not be unduly

influenced by the fact that it is merely a "voluntary" process. Given that DHS strongly encourages entities to go through the PS-Prep certification process, along with recent decisions regarding liability following an act of terrorism, entities should carefully consider what they must do now in order to plan for emergency situations.

Since 9/11, the liability landscape has dramatically changed for entities following disastrous events, particularly including acts of terrorism. Now entities are faced with the reality that an act of terrorism could be held to be a foreseeable event, and that duties are owed to third parties to protect them from the consequences of terrorist attacks. As such, whether an entity has taken measures to protect the population from terrorist attacks and other hazards, as well as whether it has undertaken measures to deter such events, mitigate their impact, and recover quickly from them will undoubtedly be examined in greater detail. Critically, the failure to undertake some or all of those actions could significantly damage any defenses tendered during litigation.

Perhaps the most salient example here is the litigation that arose out of the 1993 World Trade Center attack. *Nash v. Port Authority of New York and New Jersey, 51 App. Div. 3d 337 (N.Y. App. Div. 2008).* There, plaintiffs argued that the Port Authority of New York and New Jersey had failed to properly protect third parties from the consequences of a terrorist attack. The defendants argued strenuously that the terrorist attack was not foreseeable and that, even if it were, they were not under any duty to take precautions against its occurrence.

The jury and appellate court in this case strongly disagreed, and in fact held the Port Authority 2/3 liable for damages while the terrorists were held only 1/3 liable. It was also found that if property owners knew or should have known they were under threat from terrorists, they would have to take reasonable precautions against terrorists. Finally, in the appellate decision, the court noted that "a jury could have fairly concluded that the adoption by the defendant of the most decisive of the consultants' target-hardening recommendations would not have been ... unduly onerous." *Nash, 51 A.D. 3d at 349.*

The message from that decision is clear: If an entity knows or should know that it is under a threat from terrorist attack, it has to take measures to protect against terrorism. It is no small leap in logic to consider then that one of the first areas examined by plaintiffs' counsel is whether the defendant followed the appropriate standard of care as it related to emergency preparedness and response. In determining what exactly is the standard of care, plaintiffs will undoubtedly look to existing standards and guidelines, including those promulgated by government at all levels. In other words, in addition to existing life safety and emergency preparedness requirements, plaintiffs will certainly look to see whether the defendant had participated in or met the requirements of "voluntary" or "suggested" programs like PS-Prep. Defendants who have not participated in such programs are likely to have to offer compelling reasons as to why not. This is especially true for PS-Prep, given the thorough vetting process it uses and the fact that DHS is strongly encouraging the private sector to participate in the program.

Whether to Participate

Obviously then, such issues would make any private entity (especially those not already regulated by DHS under laws like the Chemical Facility Anti-Terrorism Standards program) consider the benefits of the PS-Prep certification program more carefully. Still, not every entity will want to take advantage of the PS-Prep program, as it might not be a good fit or could result in unduly onerous costs. In such cases, private entities might want to explore alternative avenues for liability protection, such as increased insurance limits or the liability protections offered by programs such as the Support Anti-Terrorism By Fostering Effective Technologies Act ("SAFETY Act," *6 U.S.C. §§ 441* to *444*).

In any case, the simple truth is: Courts have demonstrated a willingness to hold private entities to a higher standard when it comes to preparations for a disaster (including terrorist events), and the increasingly widespread availability of carefully considered preparedness standards makes it more likely that entities will have to take some form of action. By not doing so, they run the risk of significant liability following an event.

RELATED LINKS: For more on potential liability, see

- Homeland Security Deskbook 5.03.

For more on the SAFETY Act, see
- Homeland Security Deskbook 8.12.

Also visit Mr. Finch's commentary on using SAFETY-Act-approved products and services for site security plans under CFATS,
- 2009 Emerging Issues 4120.

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

ABOUT THE AUTHOR(S):

Brian Finch is a partner at the law firm Dickstein Shapiro LLP, where he also serves as the head of the firm's homeland security practice. He is a member of the American Bar Association's Homeland Security Executive Committee for the Administrative Law Section. Brian also serves as a Professorial Lecturer in Law at The George Washington University Law School, where he co-teaches Homeland Security Law and Policy. Brian received his B.S. from Cornell University, his M.A. from The George Washington University's Elliott School of International Affairs, and his J.D. from The George Washington University School of Law. Brian can be reached at finchb@dicksteinshapiro.com or at 202-420-4823.

4 of 19 DOCUMENTS

U.S. Corps of Engineers' Liability for Levee Breaches During Hurricane Katrina

2009 Emerging Issues 4758

BACKGROUNDER: U.S. Corps of Engineers' Liability for Levee Breaches During Hurricane Katrina

By Publisher's Editorial Staff

December 24, 2009

SUMMARY: News that a federal judge has ordered the U.S. Army Corps of Engineers to pay more than $700,000 for its role in the breaching of levees in Hurricane Katrina, causing damage to some plaintiffs, may have stunned people -- those who see a chance to recover for their losses, and those worried that they will be sued. But the facts may make this a unique case, as this article explains.

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

ARTICLE: Introduction:

Hurricane Katrina caused massive damage and set off massive litigation, but one case stands out. The U.S. District Court for the Eastern District of Louisiana has ordered the United States to pay more than $700,000, plus interest and costs, to several property owners for damage they suffered from Katrina. n1 The judge determined that the U.S. Army Corps of Engineers failed in its duties regarding the Mississippi River Gulf Outlet in several ways and that these "defalcations," as the judge often called them, led to the breaching of levees and flood damage to the plaintiffs' properties. Therefore, the judge found the United States liable under the Federal Tort Claims Act. n2

The implications for the many other people who could use this case to recover for their own losses are manifest. So are the potential costs to the government. Can this decision apply in other circumstances? If so, the repercussions could be gigantic for the many other potential government defendants. But based on the extent of what the court found that the Corps did and did not do, it seems unlikely that other governmental defendants would be endangered by this result. The opinion is long and difficult to read, so a summary is called for.

Factual Background:

The Mississippi River Gulf Outlet (MRGO) was authorized in the 1950s n3 and construction finished in 1968. The purposes were to expand the New Orleans port facilities and to shorten the route from the Gulf of Mexico to New Orleans by providing a deep passageway. The Corps of Engineers also recommended, and Congress approved, the Lake Pontchartrain and Vicinity Hurricane Protection Plan, including a "Barrier Plan." Part of the barrier plan involved

levees, which failed, leading to this litigation.

During the half-century between the beginning of the MRGO and Katrina, the Corps of Engineers generated numerous documents about the condition of the MRGO and the risks from hurricanes. The court extensively discussed this documentation, as well as other evidence and testimony. The bench trial lasted nineteen days.

Among the court's findings were:

. By the early 1970s, the Corps realized that "the MRGO was endangering" one levee, because of wave wash as ships passed. "As to the north shore, the callous and/or myopic approach of the Corps to the obvious deleterious nature of the MRGO is beyond understanding." n4

. Increased salinity changed the nature of the vegetation that provided more protection against floods (larger, denser being better). By 1962, the Corps knew of this issue and a problem from "high velocity currents caused by the MRGO." n5

. In digging the MRGO, the Corps removed almost 2,700 acres of marshland and covered other land with it - a total of almost 15,000 acres affected. This caused about 4,800 acres more to erode by 2002. Consequently, the Corps had to constantly dredge to remove the eroded debris from the channel. By July 2004, an estimated thirty-million-plus cubic yards of material had been dredged in one stretch. In 1996, the Corps described "the severe nature of bank erosion, the exponential rate of loss of marshland, and that continued erosion threatened to produce large breaches," according to the court. n6

. Although the Corps knew that the MRGO went through "malleable and shifting" soil, it did not do enough to counteract or correct the resulting lateral displacement. The result was that levees sunk, their protective berms were reduced, and the open water over which storms could travel and gain strength increased. Vegetation also was lost, which again increased the danger. n7

Ultimately, the court rejected the Corps' theory that a key levee eroded from the back. Instead, it was n8

utterly convinced that the Corps' failure to provide timely foreshore protection doomed the channel to grow to two to three times its design width and destroyed the banks which would have helped to protect the Reach 2 Levee from front-side wave attack as well as loss of height. In addition, the added width of the channel provided an added fetch which created a more forceful frontal wave attack on the levee.

As a matter of law, the court rejected the Corps' argument that the Flood Control Act of 1928, *33 U.S.C. §702c*, protected it from suit. The court had so ruled earlier in the case, and it had become "even more convinced of the validity of its decision in this regard," because the MRGO was not a flood-control measure, unlike the Lake Pontchartrain and Vicinity Hurricane Protection Plan. n9 Likewise, the court followed its previous analysis of the application of the Federal Tort Claims Act. n10 Specifically, it ruled that there was no "due care" to allow the due-care exception, n11 and the discretionary-function exception did not protect the Corps' actions (and inaction). n12

Based on the foregoing, clearly, the Corps's actions do not satisfy the second prong of the discretionary function. Clearly, the Corps failed to maintain and operate the MRGO in a manner so as not to be a substantial factor in the destruction of the Reach 2 Levee. In addition, it failed to take action that it could have taken to place foreshore protection using the very operation and maintenance funds which proved to be sufficient to fund these actions in the 1990s. Instead, it ignored the safety issues for the inhabitants of the region and focused solely on the maritime clients it serviced so well. Furthermore, the Corps failed to inform Congress of the dangers which it perceived and/or should have perceived in the context of the environmental damage to the wetlands caused by the operation and maintenance of the MRGO; in no manner can that decision be shielded by the discretionary function exception. Although the Government has introduced evidence that certain Louisiana congressman as well as other officials had knowledge of certain problems with respect to the MRGO, such general knowledge does not alleviate the Corps' professional duty and

obligation to give a specific and detailed accounting of the potential for catastrophe that could occur by virtue of the continual deterioration caused by the MRGO. In the event the Corps' monumental negligence here would somehow be regarded as "policy" then the exception would be an amorphous incomprehensible defense without any discernable contours. Therefore, there is substantial cause to find the discretionary function exception is inapplicable in this instance. n13

In particular, the court ruled that the Corps violated its obligations under the National Environmental Policy Act of 1969 (NEPA) n14 by

- Issuing a "fatally flawed" Final Composite Environmental Statement for Operation and Maintenance Work on Three Navigation Projects in the Lake Borgne Vicinity Louisiana (FEIS) in 1976,
- Not filing a Supplemental Environmental Impact Statement (SEIS) even though it acknowledged that the MRGO's operation and maintenance caused "substantial changes," and
- Improperly breaking up its reporting so that "the drastic effects the channel was causing" were harder for anyone who might read the reports to appreciate. n15 For example, the Corps did twenty-six "environmental assessments" between 1980 and 2004, each of which found no significant environmental impact. But based on various reports in evidence, the court believed that the cumulative impact of the operation and maintenance of the MRGO was significant. n16

The court pointed out, for example, that the "top-width" of the MRGO grew from its original 600 feet to be 1500 feet in 1987. n17 The court declared:

Certainly, the exponential increase in the width of the channel caused by erosion brought about by wave wash and the Corps' failure to provide foreshore protection in a timely manner constitute "significant" changes in the environment which triggered the Corps' obligation to file a more complete FEIS in 1976, file a SEIS subsequent to that, perhaps earlier but on no account later than 1988. Moreover, it is clear the Corps knew for a substantial period of time that there were "significant new circumstances or information relevant to environmental concerns and bearing on the proposed action or its impacts." *40 C.F.R. § 1502.9(c)(1)*. A review of the evidence presented leads this Court to believe that the Corps was obdurate and arbitrarily and capriciously violated its NEPA mandate. Clearly, where an agency's own findings and reports demonstrate a positive belief and objective recognition that the environmental impact of a project that requires on-going action, such as dredging for its maintenance, has created a new detrimental circumstance, such as the decimation of an extremely large swath of wetlands, a SEIS would be mandated. Furthermore, the utter failure to ever properly examine the effects of the growth of the channel on the safety of the human environment violates NEPA. For all of these reasons, the Corps does not have the benefit of the discretionary function exception. n18

...

Clearly, when there is not a mandate, if the decisions at issue are based on policy, the discretionary function exception generally applies. It is the Court's opinion that the negligence of the Corps, in this instance by failing to maintain the MRGO properly, was not policy, but insouciance, myopia and shortsightedness. For over forty years, the Corps was aware that the Reach II levee protecting Chalmette and the Lower Ninth Ward was going to be compromised by the continued deterioration of the MRGO, as has been exhaustively discussed in this opinion. The Corps had an opportunity to take a myriad of actions to alleviate this deterioration or rehabilitate this deterioration and failed to do so. Clearly the expression "talk is cheap" applies here. In the event the gross negligence of the Corps in maintaining the MRGO would be regarded as policy, then the discretionary function exception would swallow the Federal Torts Claim Act leaving it an emasculated statute applying to automobile accidents where government employees are involved or medical malpractice where a government physician is involved. This was clearly not the intent of Congress. Safety concerns are not a talisman in deciding whether to apply the discretionary function exception, but certainly are a very significant consideration. Here, there was no balancing or weighing of countervailing considerations. The failure to maintain the MRGO properly compromised the Reach 2 Levee and created a substantial risk of catastrophic loss of human life and private property due to this malfeasance. Nothing the Corps has introduced into evidence tips the

balance in its favor. n19

The court then found that these derelictions caused damage to some of the plaintiffs. Applying Louisiana law, the court explained that the Corps had a "manifestly evident ... duty not to negligently expose the levee system ... to harm" and that clearly harm to the levee system would risk damage to people and property. n20 It added that the breach of the duty of care was obvious and that "catastrophic damages" resulted from that breach. n21

Finally, the court calculated damages for each plaintiff or set of plaintiffs, finding none for some and as much as $317,000 for another. The total was $719,698.25, plus costs. Interest would run from the date of the judgment.

Return to Text

n1 *In re Katrina Canal Breaches Consolidated Litigation, 2009 U.S. Dist. LEXIS 107836* (E.D. La. Nov. 18, 2009).

n2 *28 U.S.C. § 2671*.

n3 Pub. L. No. 84-455, *70 Stat. 65 (1956).*

n4 *2009 U.S. Dist. LEXIS 107836*, at *305.

n5 *Id.* at *308.

n6 *Id.* at *316-18.

n7 *Id.* at *321-35.

n8 *Id*. at *396.

n9 *Id.* at *400.

n10 *Id.* at *402.

n11 *Id.* at *410-11.

n12 *Id.* at *411-53.

n13 *Id*. at *452-53.

n14 *42 U.S.C. §§ 4321-4370f.*

n15 *2009 U.S. Dist. LEXIS 107836*, at *476.

n16 *Id.* at *473.

n17 *Id*. at *410 (ordered to be 38 feet deep and 500 feet wide; 600 feet wide at the Gulf of Mexico), *485.

n18 *Id*. at *490-91.

n19 *Id*. at *496-97.

n20 *Id*. at *499.

n21 *Id*. at *499-500.

RELATED LINKS: See also

- In re Katrina Canal Breaches Consolidate Litigation, 627 F. Supp. 2d 656 (E.D. La. 2009) (earlier opinion in on same issues in same case)

as well as

- Ackerson v. Bean Dredging, LLC, 2009 U.S. App. LEXIS 25891 (5th Cir. Nov. 25, 2009) (dredgers have government-contractor immunity).

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

ABOUT THE AUTHOR(S):

The author is a lawyer-editor who is member of LexisNexis Matthew Bender's Immigration-Homeland Security-Admiralty practice area team.

5 of 19 DOCUMENTS

Permanent Global Entry Program: Expedited Clearance for Trusted Air Travelers

2009 Emerging Issues 4698

Jason Klitenic on Establishment of a Permanent Global Entry Program: Expedited Clearance for Trusted Air Travelers

By Jason Klitenic

December 8, 2009

SUMMARY: A chief mission and continuing challenge for DHS is to prevent dangerous people from entering our country without stifling travel and commerce. Accordingly, DHS recently proposed to make the pilot program called Global Entry permanent. Global Entry is designed to expedite the international arrival process for trusted air travelers. Jason Klitenic describes how to handle the application process and problems that may arise.

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

ARTICLE: Jason Klitenic on Establishment of a Permanent Global Entry Program: Expedited Clearance for Trusted Air Travelers

Introduction

A chief mission and continuing challenge for the U.S. Department of Homeland Security (DHS) is to prevent dangerous people and things from entering our country without stifling the free flow of travel and commerce. Consistent with these efforts, DHS on November 19, 2009, published a new proposed rule that would establish a permanent Global Entry program designed to expedite the international arrival process for trusted air travelers at U.S. airports. n1

Global Entry, which is currently implemented as a pilot program at twenty U.S. international airports, relies upon biometric identification n2 to authenticate the identity of enrolled travelers. This voluntary U.S. Customs and Border Protection (CBP) program is important because it enables DHS to pre-clear the vast majority of air travelers who are benign, while pragmatically shifting security resources to assessing higher-risk individuals who warrant tighter scrutiny.

Under the program, prescreened members arriving at U.S. airports may use kiosk fingerprint authentication to bypass the traditional CBP passport-control line. As discussed below, while the Global Entry program provides practical convenience to those who gain admission to it, the largely straightforward enrollment process can nonetheless present some notable challenges for applicant and practitioner alike.

Genesis of the Global Entry Program

The preamble of the Global Entry proposed rule cites § 7208(k) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), n3 which mandated that the Secretary of Homeland Security create an international registered traveler program designed to expedite the clearance of prescreened travelers into the United States. In so directing the Secretary, Congress expressly relied upon the report of the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission) and found that

(A) Expediting the travel of previously screened and known travelers across the borders of the United States should be a high priority.

(B) The process of expediting known travelers across the borders of the United States can permit inspectors to better focus on identifying terrorists attempting to enter the United States. n4

In response to IRTPA, CBP initiated Global Entry as a pilot program at three airports in June 2008 and ultimately expanded the pilot to twenty U.S. major international airports in August 2009. n5 The proposed Global Entry rule would transform Global Entry from a pilot program to a permanent one, while also allowing CBP to institute Global Entry at U.S. international airports beyond the twenty that currently provide it.

Program Benefits

Under the program, prescreened members arriving in the United States may use automated kiosks to facilitate their entry into the country. Rather than waiting in a traditional CBP passport-control line, a participant uses a Global Entry touch-screen kiosk to present a machine-readable U.S. passport (or lawful permanent resident card, also known as a "green card"), submit fingerprints for electronic identification, and make a customs declaration. n6 The fingerprints are compared with the member's fingerprint biometrics on file with CBP to confirm that the individual is a program participant. The participant also looks into a camera that takes a digital photograph. After the member successfully completes these steps, the kiosk generates a transaction receipt that the participant presents, along with his passport, to a CBP Officer for examination and entry. n7

DHS estimates that the Global Entry program has grown to 27,000 members and that CBP has processed approximately 100,000 entries. According to DHS, the Global Entry program has reduced average airport international entry wait times by more than 70% and more than 75% of travelers using Global Entry were processed in fewer than five minutes. n8

Eligibility and Enrollment Process

To be eligible for admission to the Global Entry program, an applicant must be at least fourteen years old and a U.S. citizen, U.S. national, or U.S. lawful permanent resident. Citizens of other countries could later become eligible for the program if CBP enters into reciprocal trusted-traveler agreements with foreign governments. n9 Based on risk factors, an applicant may be ineligible if he:

- provides false or incomplete information;
- has any prior arrests or is the subject of an investigation;
- has been found to be in violation of any customs, immigration, or agriculture laws of any country;
- is inadmissible under U.S. immigration law;
- is on a government watch list; or
- is otherwise not a low-risk traveler. n10

Those who seek admission to the Global Entry program must apply through the Global On-line Enrollment System (GOES) and pay a $100 fee. n11 The on-line questionnaire seeks personal identifier information that enables the government to check through various databases the background of the applicant to determine, among other things, whether any of the above risk factors are present. Applicants who successfully complete the on-line application process are later interviewed in person by a CBP Officer who confirms whether the candidate is eligible to become a member of the Global Entry program.

Subsequent to the interview, CBP notifies the applicant whether he has been accepted. CBP provides denied applicants with instructions regarding how to seek additional information and redress. n12

Redress and Practice Pointers

The Global Entry program has certain specific redress procedures. In short, an individual whose application has been denied may

- send a letter to the CBP enrollment center where the interview was conducted, setting forth the basis for the challenge of the denial;
- contact the DHS Travelers Redress Inquiry Program (DHS TRIP); and
- contact the CBP Trusted Traveler Ombudsman. n13

As a practical matter, the burden of proof is on the applicant to establish that he is eligible for admission to the program. Accordingly, it is important to submit accurate and complete information in the first instance; otherwise the applicant subjects himself to approval delay, application denial, or worse. Although this admonition certainly applies anytime information is provided to a law enforcement agency such as DHS, it is important to bear in mind that the government may possess more information regarding the applicant's suitability than the applicant himself has, or information that the applicant might not readily recall during the application process. Therefore, it is important to view the application process as a serious, thorough, and necessary exercise.

Problems can nonetheless arise even where the applicant views himself to have been completely forthcoming. For example, an applicant might receive a letter from CBP simply indicating that his application was denied because of a "violation of customs law," a violation that the applicant does not recall. In this possible scenario, the denial notice might not identify the particular law deemed to have been violated or when or even where the violation occurred.

In this example, one viable option would be to work collaboratively with CBP -- including submitting a Freedom of Information Act (FOIA) request -- to ascertain the basis of the denial and provide additional supporting documentation demonstrating suitability. The FOIA documents might reveal that the applicant was erroneously flagged in a database because of mistaken identity.

Unfortunately, the government's own records might shed no additional information on the alleged violation, including the particular law allegedly violated, whether any arrest or detention ensued, and where or even when the violation occurred. In instances where there is no information anywhere regarding a flag in the system (e.g., no evidence of charging documents, arrest warrant, or other legal action) it might be possible to work with CBP to establish the applicant's suitability by providing information sufficient to demonstrate that, notwithstanding the instant unexplained record notation, the applicant has had no brushes with law and presents none of the risk factors articulated in the Global Entry rule.

Because securing U.S. borders is CBP's first priority, and we are a safer nation for it, CBP does not lightly overturn denied applications to Global Entry program. Experience has shown, however, that CBP has taken a rational approach to operating its Global Entry trusted-traveler program. CBP largely affords applicants sufficient opportunity to address government concerns and present information demonstrating suitability.

In Closing

The Global Entry program proposed rule evidences DHS's continued focus and priority on security while recognizing the important interests of travel and commerce that are vital to our country. n14 The program provides substantial benefits to international air travelers, and those who apply for admission should do so in a considered and thorough fashion.

Return to Text

n1 *74 Fed. Reg. 59932* (proposed Nov. 19, 2009).

n2 For more on biometrics generally, see Sean O'Connor, Biometrics and Identification After 9/11, 7 Bender's Immigration Bulletin 159 (Feb. 15, 2002); Sean O'Connor, *Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification*, 3 Bender's Immigration Bulletin 1245 (Dec. 15, 1998).

n3 Pub. L. No. 108-458, *118 Stat. 3638, 3822 (2004)*, amended by Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, div. E, § 565, *121 Stat. 2091 (2007)*, codified at *8 U.S.C. § 1365b*. See the Global Entry proposed rule at *74 Fed. Reg. 59932* for discussion of IRTPA and trusted-traveler programs.

n4 *8 U.S.C. §1365b(k)(1)*.

n5 *74 Fed. Reg. 39965* (notice Aug. 10, 2009).

n6 *74 Fed. Reg. 59932, 59936* (proposed Nov. 19, 2009).

n7 *Id*.

n8 See DHS Press Release, Secretary Napolitano Announces Rule Proposing Permanent Global Entry Program (Nov. 19, 2009), *available at* http://www.dhs.gov/ynews/releases/pr_1258657984894.shtm.

n9 For example, under the Global Entry pilot program CBP executed a trusted-traveler agreement with the Netherlands so that Netherlands citizens who are members of that country's Privium expedited-travel program could be eligible for Global Entry. *74 Fed. Reg. at 59934*.

n10 *74 Fed. Reg. at 59934.*

n11 GOES may be accessed at http://www.globalentry.gov.

n12 *74 Fed. Reg. at 59934.*

n13 *Id*.

n14 Even more recent statements of the need for the balance are in the Declaration of Principles DHS released December 7, 2009, after a meeting between Secretary Napolitano and Mexico's Secretary of Finance and Public Credit, available at http://www.dhs.gov/xlibrary/assets/us-mexico_declaration_of_principles.pdf (last visited Dec. 8, 2009). There are countless other examples.

RELATED LINKS: Related information is at
- 8 C.F.R. 235.1(4);
- 22 C.F.R. 53.2(4).

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

ABOUT THE AUTHOR(S):

Jason Klitenic (http://www.klitenicrobertson.com/) is a founding member of Klitenic Robertson PLLC and KR Security LLC. He is Vice Chair of the American Bar Association's Committee on Homeland Security and National Defense. From 2003 to 2005 Mr. Klitenic served as the Deputy General Counsel of the United States Department of Homeland Security. In 2005 he was appointed DHS acting General Counsel and served as the chief legal officer of the 180,000-employee agency. From 2002 to 2003 Mr. Klitenic served as Deputy Associate Attorney General of the United States Department of Justice. In addition to his public service, Mr. Klitenic has been a partner at two national law firms. He also is a contributor to the Homeland Security Deskbook published by LexisNexis Matthew Bender. Mr. Klitenic received his J.D. from the University of Baltimore and B.A. from Johns Hopkins University. He is admitted to practice in the District of Columbia and Georgia.

DHS to Audit Critical Infrastructure Companies for Immigration Law Compliance

2009 Emerging Issues 4634

U.S. Department of Homeland Security to Conduct Immigration Law Compliance Audits at Critical Infrastructure Companies

By Brian Finch

November 24, 2009

SUMMARY: The U.S. Department of Homeland Security announced in November 2009 that it was set to audit nearly 1,000 companies for their compliance with requirements of the I-9 employment verification system mandated by federal immigration laws. Companies not accustomed to dealing with ICE may face close scrutiny. Brian Finch of Dickstein Shapiro explains what may lie ahead for these companies, including civil penalties and even criminal charges.

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

ARTICLE: Audits could lead to civil penalties and criminal charges

U.S. Immigration and Customs Enforcement (ICE), a component of the U.S. Department of Homeland Security (DHS), announced on November 19, 2009, that it was set to audit nearly 1,000 companies for their compliance with requirements of the I-9 employment verification system mandated by federal immigration laws. n1 These audits represent a new twist in worksite enforcement, since ICE has selected companies based on their "*connection to public safety and national security -- for example, privately owned critical infrastructure and key resources*." n2 Practically, this means that companies not accustomed to dealing with ICE are about to face close scrutiny, n3 and failures in compliance discovered during the audit could lead to civil penalties and even criminal charges.

A company that falls within the DHS definition of critical infrastructure and key resources (CI/KR) must be prepared for the possibility of an ICE audit. n4 If a company receives a letter from ICE indicating that it will be audited (officially termed a "Notice of Inspection" or "NOI" n5), it should immediately prepare for the audit as well as any fines or litigation (whether civil or criminal) that could result. This would include having the company's general counsel's office or outside compliance counsel become immediately engaged in the process.

Based upon a combination of investigative leads and ties to public safety and national security, ICE selected nearly 1,000 companies to receive NOIs. n6 Because of the "law enforcement sensitive" nature of the audits, ICE has declined to make available a list of the companies selected for audit at this time. What is clear, however, is that ICE has decided to undertake enforcement actions against segments of the economy that are not accustomed to being scrutinized for compliance with immigration laws. "Critical infrastructure" facilities like utilities, high-tech manufacturing facilities, and chemical plants are certainly accustomed to government oversight in areas related to cyber security and physical

security, but the focus undertaken by DHS now is unusual and will place untold extra burdens on their owners/operators.

The reason for the scrutiny and the close audits is relatively straightforward at this point. Specifically, ICE considers compliance with immigration laws and I-9 requirements in particular to be a major priority. It may be that the Obama administration views ICE's worksite enforcement as a key component of its interest in moving forward with Comprehensive Immigration Reform during Obama's first term, and that launching audits on previously under-inspected locations will serve as a clear message about the importance of compliance. Indeed, ICE Assistant Secretary John Morton stated that "ICE is focused on finding and penalizing employers who believe they can unfairly get ahead by cultivating illegal workplaces," and added that ICE is "increasing criminal and civil enforcement of immigration-related employment laws and imposing smart, tough employer sanctions to even the playing field for employers who play by the rules." n7

ICE's own enforcement statistics indicate just how seriously it is taking this process. Since April 30, 2009, audits by ICE have resulted in:

- 45 businesses and 47 individuals debarred (compared to 0 businesses and 1 individual debarred during the same period in FY 2008).
- 142 Notices of Intent to Fine (NIF) totaling $15,865,181 (compared to 32 NIFs totaling $2,355,330 in all of FY 2008).
- 1,897 cases initiated (compared to 605 cases during the same period in FY 2008). n8

ICE audit issues

The audits involve a comprehensive review of Forms I-9, in conjunction with a comparison to an employer's payroll records and an analysis of any technical or procedural failures n9 in I-9 completion as well as a review of any discrepancies or suspect documents on each Form I-9. All employers are required to complete and retain the Form I-9 for each individual hired in the United States. n10 Form I-9 requires employers to review and record each individual's original identity and work eligibility document(s) and determine whether the document(s) reasonably appear(s) to be genuine and related to that specific individual. The ICE audit proceeds regardless of whether the employer participates in E-Verify, and employers participating in E-Verify have been both fined and criminally charged. n11

Following the audit, ICE can issue an employer a Compliance Letter (Notice of Inspection Results, communicating a finding that the employer is in compliance) or a NIF (NIFs are charging documents, which typically relate to knowing violations, substantive violations, or uncorrected technical violations). In addition, ICE can issue intermediate notices, identifying suspect documents, discrepancies, technical or procedural violations, and warnings of violations. n12

When ICE decides to issue a NIF and go forward with fine proceedings, ICE calculates a "violation percentage" based on the ratio of violations to the number of employees for whom a Form I-9 should have been prepared. Levied fines can range from $1,300 to $8,000 per violation. Fines can be mitigated, or aggravated, based on good faith, n13 the pervasiveness of I-9 violations, whether the employer takes the initiative to correct technical violations, and the number of unauthorized workers involved. ICE also often considers the size of the business and the worksite enforcement history of the employer in deciding fine levels. Assistant U.S. Attorneys have brought criminal cases against managers and owners of entities that have been found to engage in violations of the I-9 employment verification system under money laundering, forfeiture, and harboring statutes. n14

Return to Text

n1 Immigration and Nationality Act §274A, *8 U.S.C. §1324a*; *8 C.F.R. §274a.2(b)*.

n2 See News Release, ICE, ICE Assistant Secretary John Morton announces 1,000 new workplace audits to hold employers accountable for their hiring practices (Nov. 19, 2009), *available at* http://www.ice.gov/pi/nr/0911/091119washingtondc2.htm (last visited Nov. 24, 2009) (emphasis added).

n3 Though it is true that DHS has previously done some immigration enforcement at "critical infrastructure sites." Lory Diana Rosenberg, *Separate Opinion: Crackdown: Comprehensive Immigration Enforcement*, 11 Bender's Immigration Bulletin 601 (June 15, 2006).

n4 DHS defines critical infrastructure and key resources to include Banking and Finance; Chemical; Commercial Facilities; Commercial Nuclear Reactors, Materials, and Waste; Dams; Defense Industrial Bases; Drinking Water and Wastewater Treatment Systems; Emergency Services; Energy; Food and Agriculture; Government Facilities; Information Technology; National Monuments and Icons; Postal and Shipping; Public Health and Healthcare; Telecommunications; and Transportation Systems. For more on the concept of critical infrastructure, see §4.03 of LexisNexis Matthew Bender's Homeland Security Deskbook.

n5 An example is at Ann Allott et al., Immigration Enforcement: I-9 Compliance Handbook App. F.

n6 News Release, ICE, ICE Assistant Secretary John Morton announces 1,000 new workplace audits to hold employers accountable for their hiring practices (Nov. 19, 2009), *available at* http://www.ice.gov/pi/nr/0911/091119washingtondc2.htm (last visited Nov. 24, 2009).

n7 *Id.*

n8 *Id.*

n9 For more on technical, procedural, and substantive errors, see Ann Allott et al., Immigration Enforcement: I-9 Compliance Handbook §7.05; Ann Allott on Immigration and Customs Enforcement Raids and Employer Sanctions, *2008 Emerging Issues 758 (Oct. 2007).*

n10 Immigration and Nationality Act §274A, *8 U.S.C. §1324a*; *8 C.F.R. §274a.2(b)*.

n11 E-Verify is the DHS-preferred web-based system for verifying eligibility to work in the United States. *See, e.g.*, Ann Allott et al., Immigration Enforcement: I-9 Compliance Handbook §5.04; Harry Asatrian & Ainsley Harrell, To E-Verify or not to E-Verify, *2009 Emerging Issues 4512;* USCIS website at www.uscis.gov/E-Verify (last visited Nov. 24, 2009).

n12 Examples of some of these also are at Ann Allott et al., Immigration Enforcement: I-9 Compliance Handbook App. F.

n13 Good faith is specifically referred to in *8 U.S.C. §1324a(b)(6)* and *8 C.F.R. §274a.4*. For more, see Ann Allott et al., Immigration Enforcement: I-9 Compliance Handbook §7.05.

n14 Examples can be found at ICE's Worksite Enforcement page (Aug. 25, 2008), at http://www.ice.gov/pi/news/factsheets/worksite_cases.htm (last visited Nov. 24, 2009), and http://www.ice.gov/pi/news/newsreleases/index.htm?top25=no&year=all&month=all&state=all&topic=16 (last visited Nov. 23, 2009). See also Ann Allott et al., Immigration Enforcement: I-9 Compliance Handbook §7.02.

RELATED LINKS: More information is in

- More ICE Prosecutions Brought, 11 Bender's Immigration Bulletin 981 (Aug. 15, 2006);
- Ann Allott, Daniel M. Kowalski & Camille Griffin, Immigration Enforcement: I-9 Compliance Handbook§8.05;
- Ann Allott on Immigration and Customs Enforcement Raids and Employer Sanctions, 2008 Emerging Issues 758 (Oct. 2007);
- Charles H. Kuck & Marc R. Amos, E-Verify Employment Eligibility Verification Program, 2008 Emerging Issues 2125.

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

ABOUT THE AUTHOR(S):

Brian Finch is counsel at Dickstein Shapiro, where he focuses his practice on homeland security, federal regulatory matters, and government affairs. Particular areas of focus for him include the SAFETY Act, protection of critical infrastructure, and border and trade security. Brian is a member of the American Bar Association's Homeland Security Executive Committee for the Administrative Law Section. Brian also serves as a Professorial Lecturer in Law at The George Washington University Law School, where he co-teaches Homeland Security Law and Policy. Brian received his B.S. from Cornell University, his M.A. from The George Washington University's Elliott School of International Affairs, and his J.D. from The George Washington University School of Law.

Dickstein Shapiro is uniquely situated to assist companies that have received a NOI from ICE, or those that find themselves in a legal proceeding. Dickstein Shapiro's Immigration Law Practice has experience conducting independent

audits of both corporate policies and I-9 compliance as well as representing companies in ICE audits. Dickstein Shapiro's Homeland Security Practice has handled multiple matters before DHS, including with the National Fines Office, which will be involved in any penalty phase resulting from an audit. Dickstein Shapiro's White Collar Criminal Defense & Investigations Practice is nationally renowned. With its understanding of these issues and procedures, as well as its familiarity with companies that fall within a CI/KR sector, the firm can immediately step in to assist any company facing worksite enforcement issues or looking to get ahead of possible issues in this area.

If you have any questions, please feel free to contact Amy Nice, head of Dickstein Shapiro's Immigration Law Practice, at (202) 420-2275 or nicea@dicksteinshapiro.com, or Brian Finch, head of Dickstein Shapiro's Homeland Security Practice, at (202) 420-4823 or finchb@dicksteinshapiro.com.This article is adapted from a Client Alert by Dickstein Shapiro LLP.

7 of 19 DOCUMENTS

Hoffman on The Government's Response to H1N1 and Remaining Liability Issues

2009 Emerging Issues 4567

Measure for Measure: The Government's Response to H1N1 and Remaining Liability Issues, by Sharona Hoffman

By Sharona Hoffman

November 13, 2009

SUMMARY: The increasing number of H1N1 cases raises significant liability concerns for them.This article provides an overview of the governments legal response to the H1N1 influenza outbreak and relevant statutory provisions. It also highlights current gaps in the law and remaining concerns for health-care providers. Ms Hoffman is Professor of Law and Bioethics and Co-Director of the Law-Medicine Center, Case Western Reserve University School of Law.

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

ARTICLE: By the end of October 2009, forty-eight states were reporting widespread influenza activity. Visits to doctors, hospitalizations, and deaths related to influenza and pneumonia were increasing dramatically and were much higher than expected for this period based on past influenza patterns. n1 These trends raise significant liability concerns for health-care providers. If patient loads become unmanageable, will providers be increasingly vulnerable to medical-malpractice litigation? Can the government implement measures to protect overburdened clinicians working in exigent circumstances? This article provides an overview of the government's legal response to the H1N1 influenza outbreak and relevant statutory provisions. It also highlights current gaps in the law and remaining concerns for health-care providers.

Government Action: Federal and State Declarations of Emergency and Liability Waivers

On October 24, 2009, President Obama declared a national emergency in response to the H1N1 outbreak. n2 This declaration enabled the Secretary of the Department of Health and Human Services (HHS) to issue a waiver under §1135 of the Social Security Act n3 that modified certain requirements of Medicare, Medicaid, and the State Children's Health Insurance Program (SCHIP n4), of the Emergency Medical Treatment and Labor Act (EMTALA n5), and of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. n6

Among other changes, the waiver did the following: 1) modified certain conditions of participation and certification requirements for Medicare, Medicaid, and SCHIP to facilitate payment to service providers; 2) waived the requirement that clinicians be licensed in the state in which they are working if they have an equivalent license from a different state; 3) waived certain EMTALA restrictions on the transfer and relocation of patients who have not been stabilized; and 4) waived HIPAA Privacy Rule sanctions for certain circumstances in which providers fail to obtain a patient's consent to speak with family members or friends, fail to distribute a notice of privacy practices, or neglect to

honor a patient's request to opt out of a patient directory or to implement privacy restrictions. n7 The waiver, thus, should relieve providers' anxiety about complying with some of the more cumbersome legal requirements during the H1N1 crisis.

On April 26, 2009, HHS declared a public-health emergency for H1N1, and this declaration has since been renewed twice. n8 Pursuant to this declaration, the Food and Drug Administration (FDA) authorized emergency use of Relenza and Tamiflu antiviral medication and an H1N1 diagnostic test. The declaration shields providers from liability for failure to comply with label requirements and for use of unapproved or uncleared products. n9

One additional measure taken at the federal level is a Public Readiness and Emergency Preparedness (PREP) Act declaration. The PREP Act authorizes the HHS Secretary to issue a declaration that provides immunity from tort liability (except for willful misconduct) relating to the administration and use of "covered countermeasures," which are defined to include pandemic vaccines authorized for emergency use. n10 In September 2009 the Secretary issued a PREP Act declaration for H1N1 vaccinations that provided immunity to vaccine-program planners; those qualified to prescribe, administer, or dispense vaccines; those assisting public officials with vaccination programs; the United States; and vaccine manufacturers and distributors. n11

Finally, since April 2009, at least twelve states have issued a declaration of emergency or public-health emergency relating to H1N1. These include New York, Illinois, Ohio, Iowa, Maryland, Florida, Nebraska, Wisconsin, Maine, Texas, California, and Virginia. n12 State laws vary in their scope and content. Most address the issue of liability and immunity during declared emergencies, but the categories of individuals to whom they extend immunity and the types of immunity offered differ from statute to statute. n13

The General Liability and Immunity Landscape

The federal government and several state governments have employed the legal tools available to them to address a public-health emergency and to provide a degree of protection to health-care workers involved in emergency-response activities. I present a comprehensive overview of liability and immunity issues in *Responders' Responsibility: Liability and Immunity in Public Health Emergencies*, published in the Georgetown Law Journal. n14 Although a wide range of liability protections is available under emergency declarations that have been issued and other legal provisions, health-care providers working in the private sector must recognize that gaps exist in the current immunity scheme, which leave them vulnerable to suit even at the height of a public-health emergency.

Government entities, government employees, and unpaid volunteers enjoy extensive liability protections. Government immunity for tort claims, immunity for constitutional claims, and immunity provisions in state emergency laws and mutual-aid agreements all apply to public actors. n15 Unpaid volunteers are protected by Good Samaritan laws, volunteer-protection acts, and many state emergency laws. n16 These immunity provisions cover many emergency-response activities, with the exception of willful or reckless misconduct.

Immunity protection that applies to the government and volunteers, however, does not reach paid private employees and entities. These parties are shielded only by the specifics of the emergency declarations described above and by some state laws, and these protections are limited in scope.

Liability Concerns for Private Health-Care Providers

The measures implemented by the Obama administration alleviate some but not all liability concerns for the private health-care sector. Providers will not be sanctioned for certain violations of the HIPAA Privacy Rule, EMTALA, state licensure requirements, and Medicare, Medicaid, and SCHIP procedures, as specified in the §1135 waiver. Those involved in manufacturing, administering, or dispensing H1N1 vaccines are protected by the PREP Act declaration. Similarly, some immunity is available in connection with use of H1N1 diagnostic tests, Tamiflu, and Relenza pursuant to the FDA's mandate.

In addition, state law may provide further immunity. For example, California establishes liability protection for physicians and surgeons (including those licensed in a different state), hospitals, pharmacists, nurses, and dentists who render services during a state of emergency and who are not guilty of willful acts or omissions. n17 Maine offers immunity from civil liability to private institutions and their employees and agents to the extent immunity is available to state actors for activities relating to reporting, confining individuals, and providing prescribed care during a declared extreme public-health emergency. n18 Wisconsin law establishes that persons who provide "equipment, materials, facilities, labor, or services" are not liable for death, injury, or property damage, so long as they acted under the direction of governmental authorities during a declared public-health emergency, though no immunity is available for "reckless, wanton, or intentional misconduct." n19

It is very important that health-care providers or their attorneys consult both federal and state law to determine their liability vulnerabilities. Because most states have not yet declared emergencies and because federal law is limited in the immunity it can offer private clinicians, providers should not be complacent about their liability risks. Providers caring for patients with influenza may be vulnerable to claims under a variety of theories. These include medical malpractice, corporate negligence, privacy-related torts, federal and state disability-discrimination laws, and criminal statutes. n20

Medical-malpractice claims may be of particular worry to clinicians. However, the success of such claims will depend on a determination of whether a provider violated the standard of care. This standard is based on the care a reasonable practitioner would be expected to provide under similar circumstances. The standard of care, therefore, is flexible and fact specific. n21 Juries and judges may find that the treatment clinicians are expected to give in the midst of crisis, when emergency rooms are filled well beyond normal capacity and resources are scarce, is different from the care expected during ordinary times. The fact that their conduct will be judged based on a "reasonable person" standard will undoubtedly benefit providers facing disaster-related allegations.

Nevertheless, private providers have no guarantee that they will escape liability if challenged by plaintiffs who are unhappy with the care they received. Attorneys should carefully study federal and state law as well as all emergency declarations implemented by the federal and state governments in order to advise their clients appropriately. In the absence of comprehensive legislation addressing emergency-related liability and providing further immunity protections, clinicians are right to remain concerned about potential lawsuits, and the current H1N1 pandemic may well lead to an increased volume of litigation.

Return to Text

n1 Centers for Disease Control and Prevention, 2009 H1N1 Flu: Situation Update, http://www.cdc.gov/H1n1flu/update.htm (last visited Nov. 11, 2009).

n2 Declaration of a National Emergency with respect to the 2009 H1N1 Influenza Pandemic, *available at* http://www.politico.com/static/PPM145_memo_one.html (last visited Nov. 11, 2009).

n3 *42 U.S.C. § 1320b-5*.

n4 *42 U.S.C. § 1397aa* et seq.

n5 *42 U.S.C. § 1395dd*.

n6 *45 C.F.R. §§164.510*, *164.520*, *164.522*; Department of Health & Human Services, Waiver or Modification of Requirements under Section 1135 of the Social Security Act (Oct. 27, 2009), *available at* http://www.flu.gov/professional/federal/h1n1_1135waiver_10272009.html (last visited Nov. 11, 2009).

n7 Department of Health & Human Services, Waiver or Modification of Requirements under Section 1135 of the Social Security Act (Oct. 27, 2009), *available at* http://www.flu.gov/professional/federal/h1n1_1135waiver_10272009.html (last visited Nov. 11, 2009).

n8 News Release, Department of Health & Human Services, HHS Declares Public Health Emergency for Swine Flu (Apr. 26, 2009), *available at* http://www.hhs.gov/news/press/2009pres/04/20090426a.html (last visited Nov. 11, 2009).

n9 News Release, Food and Drug Administration, FDA Authorizes Emergency Use of Influenza Medicines, Diagnostic Test in Response to Swine Flu Outbreak in Humans (Apr. 27, 2009), *available at* http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm149571.htm (last visited Nov. 11, 2009).

n10 *42 U.S.C. § 247d-6d(i)(1)*.

n11 Department of Health & Human Services, Coverage Under the Public Readiness and Emergency Preparedness (PREP) Act for H1N1 Vaccination, http://www.hhs.gov/disasters/discussion/planners/prepact/prepact-h1n1.html (last visited Nov. 11, 2009).

n12 Arizona State University Sandra Day O'Connor College of Law, Global Legal Triage and the 2009 H1N1 Outbreak, http://www.law.asu.edu/?id=2036 (last visited Nov. 11, 2009).

n13 *See* Sharona Hoffman, *Responders' Responsibility: Liability and Immunity in Public Health Emergencies, 96 Geo. L.J. 1913, 1946-50 (2008), available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1017277 (last visited Nov. 11, 2009).

n14 *Id.*

n15 *Id. at 1937-42, 1947-51.* Mutual-aid agreements enable cooperation among various states in an emergency and provide for licensure reciprocity and immunity in particular circumstances. The Emergency Management Assistance Compact, for example, is a mutual-aid agreement that has been enacted by all states and is triggered by a gubernatorial declaration of emergency and request for assistance. Many regional mutual-aid agreements exist as well.

n16 *Id. at 1943-45, 1951-53.*

n17 Cal. Gov't Code § 8659.

n18 Me. Rev. Stat. Ann. tit. 22, § 816(1). An "extreme public health emergency" is defined as "the occurrence or imminent threat of widespread exposure to a highly infectious or toxic agent that poses an imminent threat of substantial harm to the population of the State." *Id.* at § 801(4-A).

n19 Wis. Stat. Ann. § 166.03(10).

n20 Hoffman, *supra* note 13, at 1925-37.

n21 *Id.* at 1926.

RELATED LINKS: For more information see
- Homeland Security Deskbook 7.07 (2009).

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

ABOUT THE AUTHOR(S):

Sharona Hoffman is Professor of Law and Bioethics and Co-Director of the Law-Medicine Center, Case Western Reserve University School of Law. She received her B.A. from Wellesley College; a J.D. from Harvard Law School; and an LL.M. in Health Law from the University of Houston. In 2007, she was a guest researcher at the Centers for Disease Control and Prevention (CDC). She was also a member of the Institute of Medicine's Committee on Research Priorities in Emergency Preparedness and Response for the Public Health System and is a member of the Board of Scientific Counselors for CDC Coordinating Office for Terrorism Preparedness and Emergency Response. For more information, go to http://law.case.edu/FacultyResearch/MeetOurFaculty/FacultyDetail.aspx?id=117.

The Role of Small Vessels in National Security: Is DHS Doing Enough?

2009 Emerging Issues 4521

Joan Bondareff on the Role of Small Vessels in National Security: Is DHS Doing Enough?

By Joan Bondareff

October 30, 2009

SUMMARY: How familiar are you with DHSs Small Vessel Security Strategy? Joan Bondareff of Blank Rome LLP, a recognized maritime expert, here offers her views of both the Strategy and the DHS Inspector Generals critique of it. How does the Strategy deal with the risks of waterborne IEDs, of smuggled WMD or terrorists, and of outright attacks launched from a small vessel? (Think of Mumbai, the U.S.S. Cole, and the pirates off Somalia.)

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

ARTICLE: Introduction

With thirteen million registered recreational vessels (and perhaps eight million unregistered vessels) plying U.S. waters every year, it is not surprising that the Commandant of the Coast Guard, Admiral Thad Allen, has raised the critical question as to whether these vessels are "Friend or Foe?" and, in reply to his own question, said it is "Tough to Tell." n1 But the Coast Guard and its parent organization, the Department of Homeland Security (DHS), have taken serious steps to develop a new security strategy focused solely on small vessels. A small vessel is defined as a vessel that is less than 300 gross tons and generally less than 100 feet in length. It can be a recreational, fishing, or commercial vessel for purposes of this strategy. With the exception of small commercial vessels that do meet a higher standard of security, n2 as a general rule, these vessels are not subject to SOLAS or the ISPS Code. n3

The Coast Guard, DHS, and Congress, since 9/11, initially focused on the security requirements for large vessels. n4 However, given the role small vessels played in the tragic 2000 attack on the *USS Cole* n5 and the apparent maritime link to the 2008 Mumbai attacks, n6 it is understandable that in recent years these agencies and Congress have turned their attention to small-vessel security.

This attention has resulted in the issuance by DHS of a Small Vessel Security Strategy (Strategy) in April 2008. Subsequently, in September 2009, the DHS Office of Inspector General (OIG) released a report critical of the Strategy, entitled "DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement." n7 This article reviews and discusses the 2008 Strategy, the OIG report, efforts by private entities such as the National Association of Boating Law Administrators (NASBLA) and the Passenger Vessel Association (PVA) to enhance maritime security, as well as the recent issuance by the International Maritime Organization (IMO) of nonbinding guidelines for the security of vessels that are not covered by SOLAS or the ISPS Code. The article also touches briefly on recent, relevant congressional

actions.

Review of the DHS Small Vessel Security Strategy

After hosting a 2007 Summit in Arlington, Virginia, with involved stakeholders, in 2008 DHS issued its Strategy. The Strategy initially notes the difference between the present security regimes for large and small vessels. For example, all large vessels have to submit to the Coast Guard a ninety-six-hour "Advance Notice of Arrival" and a cargo manifest/crew list within twenty-four hours of departure, and must carry the Automatic Identification System. In contrast, DHS acknowledged that it lacks centralized access to hull identification and vessel registration (owner) data with respect to small vessels, there are uneven requirements for small-vessel user certification and documentation, and there are very limited advance-notice requirements for most small recreational vessels arriving from abroad.

While acknowledging that the vast majority of small-vessel operators are legitimate, law-abiding citizens, DHS expressed its concern that small vessels could be implicated in a terrorist-related attack. As the Commandant identified in his "Friend or Foe" letter, referenced above, several serious attacks have been linked to small vessels, including the *USS Cole* attack, the October 2002 attack by a small fishing vessel with explosives into the side of the supertanker *Limburg*, and the November 2005 attack on the cruise ship *Seabourne Spirit* by terrorists using twenty-five-foot inflatable boats. n8

The Small Vessel Security Strategy identified the following four scenarios of greatest concern that small vessels could pose in terrorist-related attacks:

- "Domestic Use of Waterborne Improvised Explosive Devices (WBIEDs)";
- "Conveyance for smuggling weapons (including WMDs) into the United States";
- "Conveyance for smuggling terrorists into the United States"; and
- "Waterborne platform for conducting a stand-off attack (e.g. Man-Portable Air Defense System (MANPADS)) attacks."

As part of its strategic vision for responding to these potential scenarios, the Strategy determined that a "one-size-fits-all approach cannot adequately ensure U.S. maritime security and safety due to the diversity of the maritime domain and the heterogeneity of the small vessel community." n9 Therefore, the Strategy contains four diverse goals with specific objectives pertaining to each goal.

The first goal is to: "*Develop and leverage a strong partnership with the small vessel community and public and private sectors in order to enhance maritime domain awareness*." n10 A specific objective to address this goal is to partner with the eighty million individuals who participate in recreational boating activities each year, and to increase public awareness of how to report suspected terrorist activity through America's Waterway Watch (AWW). n11 DHS cited as a prime example of the success of AWW when a tour boat operator in Florida in 2003 reported suspicious activity by one of its passengers, which led to the investigation of the suspect and his apprehension in New York. n12

The second goal of the Strategy is to: "*Enhance maritime security and safety based on a coherent plan with a layered, innovative approach*." n13 To implement this goal, the Coast Guard will identify which operators present a low-risk profile, and develop appropriate risk-targeting systems to distinguish high-risk users. The Coast Guard also called for enhanced use of the ninety-six-hour-advance-notification rule for recreational vessels entering U.S. waters from overseas.

The third major goal is to: "*Leverage technology to enhance the ability to detect, determine intent [of], and when necessary, interdict small vessels*." n14 To achieve this goal, the Coast Guard acknowledged that it must expand research into low-cost, non-intrusive, small-vessel-identification systems, such as radio frequency identification (RFID) tags, adaptable miniature transponders, portable GPS devices, or cell-phone-based recognition systems. n15 The Coast Guard also has memoranda of understanding with States to allow access to basic information about state-registered recreational vessels through the Vessel Identification System.

The fourth and final goal of the Strategy is to: "*Enhance coordination, cooperation, and communications between Federal, state, local, and Tribal partners and the private sector as well as international partners*." n16 One way to implement this goal, according to DHS, is to update area maritime security processes to ensure that small vessels are addressed when conducting area assessments and developing area security-management plans. Another method, as the Commandant described in "Friend or Foe," is to partner with organizations such as NASBLA. He credits NASBLA with "advocating for the state registration of all motorized and non-powered vessels (canoes, kayaks, etc.)" to increase maritime domain awareness at the local and state levels. The PVA is another source of cooperation on security matters. n17

To carry the Strategy to the next phase, the Coast Guard is developing an implementation plan to provide detailed direction to all DHS agencies on how to achieve the four major goals. As of this writing, we do not have information on the date of release of the plan.

Review of the OIG Report and DHS Response

DHS OIG found the Strategy to be deficient in certain respects after comparing it with the six characteristics for an effective national anti-terrorism strategy articulated by the General Accounting Office (GAO) in its 2004 report entitled "Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism." n18 The six characteristics prescribed by GAO include: problem definition and risk assessment; goals and performance measures; identification of resources; organizational roles and responsibilities; and integration and implementation.

The OIG criticized the Coast Guard for not addressing all of the characteristics laid out in the GAO report, such as setting priorities, milestones, performance measures, or progress indicators. The OIG also criticized the Coast Guard/DHS for not providing detailed information regarding costs, human capital, resources, or economic principles. Finally, the OIG commented that DHS had not sufficiently analyzed the adequacy of certain programs and processes that DHS would rely on in support of its Strategy, such as the AWW and the Pleasure Boat Reporting System that Customs and Border Protection administers for small vessels traveling to the United States from a foreign country. OIG complained that the AWW is not widely known, that AWW calls are not tracked, and that the Pleasure Boat Reporting System is ineffective and the data it gathers not accurate.

In response, DHS partly agreed and partly disagreed with the OIG's conclusions. For example, DHS acknowledged that it could address more of the GAO characteristics and stated that it planned to do so in the execution of its implementation plan. n19 However, DHS did not concur with the OIG recommendation that it needed to evaluate the effectiveness of programs such as AWW and the Pleasure Boat Reporting System in order to use them as part of its solution to improve security from small-vessel threats, since they had been recommended by DHS agencies as useful tools. n20

Initial Assessment and Next Steps-Implementation Plan, IMO Guidelines, and Congressional Action

While it is beyond the scope of this article to fully assess either the GAO process or the OIG report, in the view of this author, the OIG report is fairly formulaic and fails to take into account the diffuse nature of the recreational boating community, the tremendous cost of administering a new security program for the eighty million Americans who enjoy recreational boating, and the seriousness of the effort that the Coast Guard and rest of DHS have undertaken in trying to develop a Small Vessel Security Strategy that balances the individual rights of boaters in this country to operate in U.S. waterways alongside other maritime partners with the damage that a terrorist attack from a small vessel of the nature described above could inflict on a waterway, port, or other critical infrastructure.

In the meantime, DHS is developing and planning to release an implementation plan to fill in a number of the gaps identified by the OIG. The Coast Guard has also worked closely with the IMO's Maritime Safety Committee to develop a set of nonbinding guidelines that can be used by government and private entities engaged in small-vessel operations and security. The IMO issued the guidelines in December 2008 to address the lack of existing guidance on security

aspects of those ships that do not fall within the scope of SOLAS and the ISPS Code, i.e., small vessels. n21 The IMO made clear that the guidance is not mandatory.

However, the author expects that a number of the guidelines will show up in the final Coast Guard implementation plan because they offer practical suggestions and best-management practices for government entities and operators alike. For example, the IMO recommended that Member States consider encouraging operators of pleasure craft to register with a suitable organization that could provide a database available for authorized online access to assist in both prevention and response activities related to both safety and security. n22 The IMO also recommended that Member States encourage operators of small vessels engaged in international voyages to adopt, where appropriate, the provisions of the ISPS Code as industry best practice. n23 Finally, the Guidance contains detailed recommendations on how small vessels can mitigate the risk of theft, piracy, and armed robbery n24-a serious new (or new old) problem, but one that is not addressed in this commentary.

Congress is watching the development of the Strategy closely. In November 2009, the House Transportation and Infrastructure Committee expects to hold a hearing on Maritime Domain Awareness, which will include a review of the Strategy. Congress has also taken steps to correct the lack of criminal penalties for operators of submersible and semi-submersible vessels that engage in international voyages without a national registry. n25 And the House of Representatives just passed the Coast Guard Authorization Act for FY2010, which includes language directing the Secretary of Homeland Security to establish a Maritime Homeland Security Public Awareness Program, encouraging recreational and commercial boaters to improve awareness of activity in the maritime domain and report suspicious or unusual activity. n26

Conclusions

DHS and specifically the Coast Guard have undertaken a serious review of the potential threat from small vessels and taken the initial steps necessary to develop a security strategy and implementation plan for that strategy. DHS acknowledged, in response to the OIG report, that it needs to do more to follow all of the recommended GAO steps for such a strategy and plans to incorporate the suggestions in the implementation plan.

The small-boating community can expect to see closer scrutiny paid to small vessels-with accompanying increased regulation and financial commitments. The movement is likely to be in the direction of more SOLAS- and ISPS-like compliance mechanisms for owners and operators of small vessels. Companies with off-the-shelf technologies that can address these issues may also find a welcome mat at the Coast Guard.

Return to Text

n1 Thad Allen, Friend or Foe? Tough to Tell, Proceedings (Oct. 2008), available at www.usni.org.

n2 The requirements for commercial small vessels are described at length in the October 2009 issue of Foghorn magazine, a publication of the Passenger Vessel Association. See www.foghornmagazine.com.

n3 The International Convention for the Safety of Life at Sea (SOLAS), adopted November 1, 1974, entered into force May 25, 1980, as amended by the International Ship and Port Facility Security Code (ISPS), which

entered into force July 1, 2004. Go to www.IMO.org/Conventions.

n4 The Marine Transportation Security Act of 2002, Pub. L. No. 107-295, *116 Stat. 2064,* was one of the first U.S. laws to address security requirements for large vessels, and is intended to implement the IMO's ISPS Code for them.

n5 Raphael Perl & Ronald O'Rourke, Congressional Research Service Report No. RS20721, Terrorist Attack on USS Cole: Background and Issues for Congress (Jan. 20, 2001).

n6 See "The United States warned the Indian government about a potential maritime attack against Mumbai at least a month before last week's massacre in the country's financial capital left nearly 180 dead, a U.S. counterterrorism official told CNN." Source: U.S. Warned India about possible Mumbai attack, Dec. 2, 2008, http://www.cnn.com/2008/WORLD/asiapcf/12/01/india.attacks2/index.html.

n7 DHS OIG-09-100.

n8 Proceedings, supra note 1, at 15.

n9 Strategy at 11, 15.

n10 Strategy at 16.

n11 www.AmericasWaterwayWatch.org.

n12 Strategy at 16.

n13 Id. at 17.

n14 Id. at 19.

n15 Id. at 20.

n16 Id.

n17 See www.passengervessel.com.

n18 GAO-04-408T (statement of Randall A. Yim to the Subcommittee on National Security, Emerging Threats, and International Relations of the House Committee on Government Reform, to be given February 3, 2004). The GAO has been rechristened the "Government Accountability Office."

n19 OIG report, supra note 7, at 17.

n20 Id.

n21 Non-Mandatory Guidelines on Security Aspects of the Operation of Vessels Which Do Not Fall Within the Scope of SOLAS Chapter XI-2 and the ISPS Code.

n22 Id., Annex at 5.

n23 Id., Annex at 6.

n24 Id., Annex at 20.

n25 The Drug Trafficking Vessel Interdiction Act of 2008, Pub. L. No. 110-407, *122 Stat. 4296.*

n26 Sec. 1101 of H.R. 3619 (2009).

RELATED LINKS: For general information on international maritime security measures, see
- Homeland Security Deskbook 10.02.

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

ABOUT THE AUTHOR(S):
Joan Bondareff is Of Counsel to Blank Rome LLP, in Washington, DC, and is a recognized expert in maritime law and regulations. Before entering private law practice, Ms. Bondareff was the Chief Counsel of the U.S. Maritime Administration and Acting Deputy Administrator; the Majority Counsel to the House Committee on Merchant Marine and Fisheries; and the Assistant General Counsel to the National Oceanic and Atmospheric Administration. Ms. Bondareff also served on the Transition Team for the Department of Transportation for the incoming Obama Administration on maritime issues. Ms. Bondareff has published extensively in this field, including such articles as: *Changes in Congress -- Changes in Store for the Maritime Industry*, 5 Benedict's Maritime Bull. 1 (2007) (co-author); The Impact of the Economic Crisis on the Shipping Industry and Trade Consequences, WIIT Newsletter (Women in International Trade), Winter 2009.

9 of 19 DOCUMENTS

SAFETY-Act-Approved Products in CFATS Site Security Plans Can Limit Liability

2009 Emerging Issues 4120

The Importance of Using SAFETY-Act-Approved Products and Services When Submitting Site Security Plans Under the Chemical Facility Anti-Terrorism Standards: The SAFETY Act Offers the Additional Benefit of Liability Protection for Your Company

By Brian Finch

August 13, 2009

SUMMARY: Brian Finch explains how to take advantage of the SAFETY Act to implement the Chemical Facility Anti-Terrorism Standards (CFATS) law, especially in creating Site Security Plans. Use of approved products and services can limit liability to lawsuits. Mr. Finch is an expert on homeland security issues, including the SAFETY Act. He practices at Dickstein Shapiro LLP and lectures at the George Washington University School of Law.

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

ARTICLE: ***The Importance of Using SAFETY-Act-Approved Products and Services When Submitting Site Security Plans Under the Chemical Facility Anti-Terrorism Standards: The SAFETY Act Offers the Additional Benefit of Liability Protection for Your Company***

When the Department of Homeland Security (DHS) began implementing the Chemical Facility Anti-Terrorism Standards (CFATS) law, n1 the prospect of undertaking the increased security requirements under the law seemed daunting. As DHS reviewed the risks posed by the 36,000 sites that completed an initial security review through the "Top Screen" process, n2 and then asked about a fifth of those facilities to submit Security Vulnerability Assessments (SVAs), n3 owners and operators became increasingly concerned about the cost of compliance. Unfortunately, with the recent release of the Risk Based Performance Standards (RBPS) and the determination of which facilities fall into the highest risk category, the compliance costs are about to significantly increase. n4

Owners and operators of facilities covered by CFATS at any level should not, however, just be worried about paying for vehicle barriers or inventory control systems. They also need to be concerned about the potential liability they could face in the event of a terrorist attack due to the fact that mere compliance with CFATS will not relieve them of any liability. The only true way to manage such liability is through the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 (the SAFETY Act). n5 Companies submitting their Site Security Plans (SSPs) n6 to DHS should remember to take advantage of the vast liability protections offered by the SAFETY Act by ensuring that the products and services chosen for the SSP are SAFETY-Act-approved technologies.

The SAFETY Act was enacted after the September 11, 2001, terrorist attacks to assure eligible companies that,

should another terrorist attack occur, they would not be exposed to uncapped legal liability. Simply put, the SAFETY Act provides companies with an opportunity to apply to DHS for certain tort liability protections in connection with the manufacture or furnishing of products or services that can be used to detect, defend against, or respond to acts of terrorism. Two tiers of protection are available under the Act.

If a product or service receives SAFETY Act "certification," then the owner, seller, and/or provider of that product or service presumptively would be entitled to immunity from all tort claims for damages arising out of an act of terrorism and associated with the product or service. n7 Alternatively, it the product or service just receives a SAFETY Act "designation," the applicant's potential tort liability would be limited to the amount of insurance that DHS determines the applicant should maintain in connection with such losses. n8 In either case, tort claims cases may be brought only in federal court. n9

Companies can take advantage of the SAFETY Act by purchasing SAFETY-Act-approved products and services. Under the Act, only "sellers" of SAFETY-Act-approved products or services potentially could be liable for damages in connection with such products or services. By contrast, mere purchasers of SAFETY-Act-approved products or services **face no liability**. n10 A wide range of products and services have received SAFETY Act protections. n11

Given such protections, owners and operators of covered facilities putting together their SSPs should think about the SAFETY Act at every turn. When purchasing barriers, fences, cameras, cyber security systems, security guards, and other products and services, covered facility owners and operators need to think about goals far beyond satisfying the RBPS specifically. Owners and operators must also think about putting together SSPs in ways that minimize their potential terror-related liability. There are several approaches to doing so, including:

- **Buy SAFETY-Act-approved products and services:** When buying security items as part of your approved SSP, look to purchase SAFETY Act approved items. Those items will give the buyer liability protections in the form of limited immunity for terror related claims. Only the SAFETY Act offers such liability protections.
- **Encourage security vendors to pursue SAFETY Act protections:** If none of the products or services in the particular market have SAFETY Act protections, and you need that item in order to implement your SSP, then ask your potential vendors to pursue SAFETY Act protections. A number of buyers of anti-terror products and services already impose such a requirement, and if the owner of a shopping mall or an airport can impose such a requirement, so too can the owner of a Tier 1 facility.
- **Think creatively about what you can cover by the SAFETY Act:** Many products that a tiered facility will have to buy as part of an approved SSP are obvious SAFETY Act candidates, such as fences, explosive detection equipment, and security guards. But there are many other areas that can receive SAFETY Act protections as well. For instance, maintenance services for detection equipment can be approved under the SAFETY Act, as can engineering design and construction services. You should be on the lookout for buying SAFETY-Act-approved items in as many areas as possible in order get the greatest amount of liability protection available.

Remember, earning SAFETY Act protections is not easy: Companies that have been through the SAFETY Act process will tell you that it is anything but a rubber-stamp exercise. DHS requires a significant amount of information on policies, procedures, and field deployment data from an applicant before it will determine that the product or service is "useful" and "effective" against terrorism, thereby meriting a SAFETY Act award. While the SAFETY Act award itself *should not* be considered a "stamp of approval," buyers can reasonably infer that an approved product or service has been thoroughly examined by DHS and that the receipt of SAFETY Act protections signals that there is significant quality associated with the product.

Companies can also consider other options like having their SSP SAFETY Act approved in order to provide an umbrella of SAFETY Act protections. The critical point, however, is that when purchasing your security products and

services in order to implement the SSP, it will be highly beneficial to take advantage of the unmatched liability protections associated with purchasing SAFETY Act-approved products and services. If you must comply with CFATS, then it only makes sense to do so in a way that also insulates you from potentially massive liability following a terrorist attack.

Return to Text

n1 Section 550 of the Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, *120 Stat. 1355, 1388 (2006).*

n2 *See generally 6 C.F.R. § 27.200*.

n3 *6 C.F.R. § 27.215*.

n4 See *6 C.F.R. § 27.230* and http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf.

n5 *6 U.S.C. §§ 441-444* (the codified version of Title VIII, subtitle G, §§ 861-865, of the Homeland Security Act of 2002, Pub. L. No. 107-296, *116 Stat. 2135).*

n6 *6 C.F.R. § 27.225*.

n7 *6 C.F.R. § 25.8*.

n8 *6 C.F.R. §§ 25.4, 25.7*.

n9 *6 C.F.R. § 25.7*.

n10 *6 C.F.R. § 25.7.*

n11 For a list of products and services that have received SAFETY Act protections, see www.safetyact.gov.

RELATED LINKS: For more information on CFATS, see
- Joe Whitley & Ed Britan on a New Standard for Security Regulation: The Interim Final Rule on Chemical Facility Anti-Terrorism Standards, 2008 Emerging Issues 2273.

For more on the SAFETY Act and on CFATS, respectively, see
- Homeland Security Deskbook 8.12;
- 11.05.

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

ABOUT THE AUTHOR(S):

Brian Finch is counsel at Dickstein Shapiro, where he heads the firm's Homeland Security Practice. Brian focuses his practice on homeland security, federal regulatory matters, and government affairs. Particular areas of focus for him include the SAFETY Act, protection of critical infrastructure, and border and trade security. Brian has developed a unique level of expertise in assisting applicants through the SAFETY Act process. He has helped draft over 100 applications for a wide variety of products and services, ranging from security guards and vulnerability assessments to software programs and security screening devices.

Brian is a member of the American Bar Association's Homeland Security Executive Committee for the Administrative Law Section. Brian also serves as a Professorial Lecturer in Law at The George Washington University Law School, where he co-teaches Homeland Security Law and Policy. Brian received his B.S. from Cornell University, his M.A. from The George Washington University's Elliott School of International Affairs, and his J.D. from The George Washington University School of Law.

Brian can be reached at finchb@dicksteinshapiro.com or at 202-420-4823.

10 of 19 DOCUMENTS

PASS ID Act: Putting the Brakes on Security Standards for Drivers' Licenses

2009 Emerging Issues 3904

Janice L. Kephart on the PASS ID Act: Putting the Brakes on Security Standards for Drivers' Licenses

By Janice L. Kephart

June 29, 2009

SUMMARY: Janice L. Kephart, former counsel to the 9/11 Commission, discusses proposed amendments to the REAL ID Act's provisions on drivers' licenses and other state-issued identification. The proposed Providing Additional Security in States' Identification (PASS ID) Act of 2009 was introduced as S. 1261. Sponsors claimed support of the National Governors Association, National Conference of State Legislators, and privacy and civil-liberties groups.

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

ARTICLE: The Obama Administration is supporting a handful of members of the Senate Committee on Homeland Security and Governmental Affairs in their attempt to repeal the driver's-license provisions of the REAL ID Act of 2005. n1 On June 15, 2009, the *Providing for Additional Security in States' Identification (PASS ID) Act of 2009* was introduced. n2 The bill's provisions repeal the key substantive provisions regarding drivers' licenses aimed at fulfilling 9/11 Commission recommendations that ensure all states meet minimum security standards in issuing drivers' licenses and other identification documents (IDs).

A 9/11 Commission Recommendation

REAL ID was enacted in 2005 in direct response to factual findings and recommendations of the 9/11 Commission. The Commission found that eighteen of the nineteen hijackers obtained seventeen drivers' licenses and thirteen state IDs, including at least seven obtained by fraud in Virginia. n3 Evidence showed that at least six of these IDs were used to help the hijackers board planes on the morning of 9/11. n4

Of the legally obtained IDs, many were duplicates, with some states issuing the same hijacker multiple licenses over a period of several months. n5 For example, airline ticket personnel recalled that at least four hijackers at Logan International Airport in Boston and two hijackers at Dulles International Airport in Virginia used state-issued drivers' licenses as their ID to board, with at least two of these IDs obtained by fraud. n6 Pentagon pilot Hani Hanjour had four IDs, all from different states, with at least one obtained by fraud. n7 The Pennsylvania pilot, Ziad Jarrah, was likely carrying his two drivers' licenses from Florida and a fraudulently obtained Virginia ID when pulled over for speeding two days prior to 9/11. n8

The Commission stated:

All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identifications would have assisted them in boarding commercial flights, renting cars, and other necessary activities.

Recommendation: *Secure identification should begin in the United States. The federal government should set standards for .. sources of identification, such as drivers licenses.*

Recommendation: *The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system-wide goals in mind.* n9

The 9/11 hijackers are not the only terrorists we know of who have taken advantage of blind spots and weaknesses in ID-issuance standards. One terrorist caught in 2001 on the northern border, Nabil al Marabh, had five drivers' licenses and a hazardous materials permit. Mir Aimal Kansi, who killed two people outside CIA headquarters in 1993, got a Virginia driver's license despite being in the United States illegally. n10

The Kansi-type problem has been reduced significantly because many states have chosen to check lawful presence through the federal Systematic Alien Verification for Entitlements (SAVE) program database in the past two years, including an emergency measure to comply with REAL ID passed by the Maryland legislature in April 2009, leaving only three states struggling with a surge in illegal alien activity in the states. n11 REAL ID has encouraged use of SAVE, as legal-status checks are a required benchmark for compliance, and the result has been a marked increase in security and reduction of fraud. However, the 9/11 and al Marabh multiple-ID problem has not been solved yet. REAL ID -- but not PASS ID -- requires states to network to assure that drivers have only one license at a time. Mississippi is taking the lead in building the network with a $17 million appropriation, but until the network is complete, anyone with an ill intent will be able to "license shop" amongst states and even, depending on the state, within a state.

American Association of Motor Vehicle Administrators (AAMVA) Technical Standards

Most of the REAL ID provisions were adopted from the 2004 Security Framework drafted by the American Association of Motor Vehicle Administrators (AAMVA) and published in a lengthy report in response to the 9/11 Commission's investigation. n12 The standards emphasized that identity documents must be secure in their content, physical features, and issuance process. Without identity security at the base of identity-document issuance, the AAMVA concluded that driver's-license-issuing standards would not produce secure licenses:

The license is now readily accepted as an official identification document for both licensed drivers, and, in most jurisdictions, for non-drivers. The Motor Vehicle Administrations (MVAs) who issue these documents have unique, continuous and long-lasting contact with most of their constituents from the individual's teenage years onward.

Most MVAs allow driver's license reciprocity with other MVAs; therefore a common security protocol among MVAs is necessary. This document provides minimum standards of security, interoperability and reciprocity agreed upon by all North American MVAs regarding driver's license/identification card (DL/ID) issuance. Each MVA shall:

- *Either meet or exceed the requirements of the Security Framework based on risk analysis and resource availability.*
- *Determine that all individuals granted a DL/ID "are who they say they are."*
- *Ensure that each individual issued a DL/ ID "remains the same person" throughout subsequent dealings .. with itself*

or any other MVA. n13

REAL ID Act of 2005

To address the 9/11 Commission's and AAMVA's recommendations, Congress enacted the REAL ID Act in 2005. The Act includes the following compliance requirements:

- **Identity verification.** Each driver's license or identity card will be required to contain a person's full legal name, signature, date of birth, gender, driver's license or identification number, photograph, and principal place of residence.
- **Document authentication.** States are required to digitize birth records (another key 9/11 Commission recommendation) and review the authenticity of the information provided to obtain a license, such as Social Security information, immigration or lawful-presence documentation, and other proof of identity, such as principal place of residence.
- **Card security.** REAL ID requires a certain level of physical-security features to ensure more tamper-proof cards.
- **Security plans.** To ensure states meet security and privacy standards and to hold them accountable, REAL ID requires states to submit detailed security plans.
- **One driver, one license.** REAL ID requires creation of a network of state databases to enable states to verify that applicants do not hold multiple licenses in multiple states, something states already do voluntarily for commercial licenses and "bad" drivers. They are also exchanging digital images of drivers outside of REAL ID requirements.
- **"Official purposes" requirement.** REAL IDs will be required to board a commercial aircraft or enter a federal building and for other uses for "official purposes."

REAL ID Regulations n14

REAL ID regulations were issued after a long comment period in January 2008, providing extending compliance deadlines for states and setting out specific benchmarks for compliance.

- Applicability. The rules require that a REAL ID is necessary for access to "official purpose areas" such as nuclear power plants and other federal facilities, as well as for boarding a commercial aircraft.
- Definitions. Key definitions include a broad definition of lawful status, which includes a pending asylum application, and personally identifiable information, such as biometrics or any information used to trace an identity.
- Validity. REAL IDs cannot be valid for longer than eight years, but can be valid for a shorter period.
- Compliance
- Consumers. All those under the age of fifty on December 1, 2014, must have REAL ID-compliant cards on that date. Those older than fifty need not be compliant until December 1, 2017. After the respective deadlines, non-REAL IDs cannot be accepted for official purposes and must indicate on their faces and in their machine-readable zones (MRZs) such unacceptability. Materially compliant cards will bear a DHS-approved security marking.
- States. All states received an extension in March 2008. States must be materially compliant with the first eighteen benchmarks no later than December 31, 2009, to receive an additional extension towards full compliance by May 11, 2011.

Benchmarks for first tier (December 31, 2009) material compliance include a certification that the state does or has the following:

(1) Mandatory facial image capture and retention of the image;

(2) *Signed declarations* under penalty of perjury *and retention of the declarations*;

(3) Required presentation by the applicant of *identity source documents*;

(4) Required documentation of date of birth, Social Security number, address of principal residence, and lawful status;

(5) A documented exceptions process in place;

(6) Reasonable efforts to ensure that an *applicant does not have more than one DL or ID card under a different identity;*

(7) *Verification of lawful status via SAVE*, the Systematic Alien Verification of Entitlements System;

(8) *Verification of the Social Security number* with the Social Security Administration (SSA);

(9) DLs with *levels 1, 2, and 3 security features* pursuant to 6 C.F.R. §37.15;

(10) Specified data on the faces of the cards;

(11) *Materially compliant DLs* marked with a DHS-approved security mark;

(12) *Temporary or limited-term licenses* issued to individuals with temporary lawful status and with validity of license to end with the lawful status;

(13) Have a documented security plan in place pursuant to 6 C.F.R. §37.41;

(14) *Security of personally identifiable information ensured*;

(15) Covered employees required to attend AAMVA or equivalent fraudulent-document-recognition training;

(16) Name- and fingerprint-based criminal-history and employment-eligibility checks on all covered employees;

(17) Commitment to material compliance by January 10, 2010, or within ninety days of submission of the certification;

(18) Clear statements on the faces of noncompliant DLs or IDs that they are not acceptable for official federal purposes.

Identity Verification and Document Authentication of the Applicant. The applicant must provide sufficient documentation for a state to both verify identity and authenticate documents presented for the purpose of establishing identity. *Identity is established by a combination of biometric (digital photo only) and verified government-issued identity documents, using technologies as they become available.* Applicants must provide the following to establish identity:

- *Facial image* -- captured prior to DL/ID issuance, and a *declaration under penalty of perjury* that the information provided is true and correct. This must be maintained by the state. ***Note:*** *Lawful status* must be authenticated by one check in SAVE. If there is a non-match, the DMV cannot issue a REAL ID until there is resolution with U.S. Citizenship and Immigration Services (USCIS).
- *Date of Birth* -- verified with any of the listed documents that also verify identity. Birth certificates should be verified through the Electronic Verification of Vital Events (EVVE) system or other DHS-approved method. If documents do not appear authentic or there is a nonmatch, no DL/ID shall be issued until there is resolution with the issuing office.
- *Social Security card, W-2, 1099 form, or other similar document* -- checked against the SSOLV (SSN match) database. If there is a nonmatch, the DMV cannot issue a REAL ID until the information is verified with the SSA.

- *Principal Residence* -- demonstrated with two documents of the state's choosing showing both name and address. (Exceptions exist, usually for safety or protection, such as for domestic violence victims or law enforcement personnel.)
- **One Driver, One License.** States must make "reasonable efforts" to ensure that the applicant does not hold multiple DLs or IDs under different identities or names. If other DLs or IDs are found, the state of application must ensure that the others have been terminated prior to issuing a new REAL ID DL or ID, by verification with the issuing state.
- **Hardening the License or ID.** A key feature of REAL ID is that the cards include "document security features .. designed to deter forgery and counterfeiting, promote an adequate level of confidence in the authenticity of cards, and facilitate detection of fraudulent cards in accordance with this section." n15 Technologies must not be commonly available to the general public, must be layered into three levels of security, and must be able to be integrated into the cards.

In addition, all cards shall bear a *DHS-approved security marking* reflecting whether the card is materially or fully compliant with DHS Rules. (This rule has been awaiting Office of Management and Budget approval since January 2009.)

- **Categories of Driver's License or ID.** REAL ID sets standards for the varieties of cards a state can issue, including temporary or limited-term (as those issued to legal residents), and reissuance and renewals, which need not occur more frequently than every sixteen years. States are free to issue non-REAL IDs as long as such drivers' licenses or IDs clearly state on their faces and in the MRZs that the DL/ID is not acceptable for official purposes.
- **Security Plan for Employees, Personally Identifiable Information, and Production Facilities**

As part of its certification, the state must submit a security plan that contains the following elements:

(1) *Physical security* of production facilities and storage areas for card stock and production.

(2) *Security of personally identifiable information* as follows: All documents presented to show identity and lawful status or other personally identifiable information shall be protected as described in the security plan, including (1) procedures to prevent "unauthorized access, use, or dissemination of applicant information and images of source documents" n16 retained under REAL ID and "standards and procedures for document retention and destruction"; n17 (2) a privacy policy; (3) and compliance with the Driver's Privacy Protection Act. n18

(3) *Document and Physical Security Features of the Card* and the state's use of biometrics.

(4) *Employee access control*, including credentialing; background checks; controlled access to systems; *fraudulent-document training;* and security-awareness training. Background checks for employees include prior employment references, name- and fingerprint-based criminal-history checks, and employment-eligibility verification. The state is "encouraged to participate in the USCIS E-Verify program." n19

(5) A separate report on how a state will safeguard identities as necessary in coordination with government and law-enforcement entities.

- **Procedures for Determining State Compliance.** States are subject to DHS audits to determine compliance, including onsite inspections and interviews of employees. Audits must be conducted within forty-five days of DHS receiving a state's certification of material or full compliance. A state can fail to comply with REAL ID by (1) failing to submit a certification or (2) failing to meet one or more of the standards in the regulations.

PASS ID Act

The primary supporters of PASS ID have made their opposition to REAL ID clear, and the PASS ID language demonstrates that their goal is to freeze standards as they are today instead of continuing to strengthen licensing under

REAL ID.

Specifically, **PASS ID would**:

Weaken identity verification. Two areas are key: ensuring that people are who they say they are (identity verification) and digitization of birth records to safeguard issuance. PASS ID returns identity verification to identity validation, the pre-9/11 standard, in which the state could simply rubber-stamp documents, such as birth certificates, principal residency documents, electronic verification of Social Security numbers, and passports. This was the same process that five 9/11 hijackers used to secure fake documents (principal residence affidavits) in Virginia, which enabled them to obtain IDs in early August 2001. REAL ID combats this problem by adding passport verification and birth-record digitization as additional layers of security. n20

Lawful presence checks are effective only if identity verification and document authentication (ensuring that documents used are valid and trustworthy) are sufficient. Absent sufficient verification, an applicant would only need to steal, borrow, or buy a legal immigrant's or U.S. citizen's identity, use it to validate submitted paperwork, and then undergo a lawful-presence screening, which is largely ineffective without the identity-verification step. In essence, these requirements would further enable identity theft, instead of combating it like the requirements of REAL ID.

Give states money without accountability or fiscal responsibility. PASS ID gives grant money to states without any accountability or any requirement to comply with the PASS ID requirements. In fact, PASS ID would not apply if a state privacy law preempts the legislation. The bill would push back the compliance deadline until 2017 (currently states would be required to be in compliance for those younger than fifty by 2014). Finally, even though most states already exceed PASS ID standards, it would not require states to demonstrate progress toward achieving the standards in exchange for the federal grants, which translates into essentially free money for states to use at their discretion. At a cost to U.S. taxpayers, the PASS ID Act also requires the federal government to provide free access to states for lawful-status-database checks, including checking Social Security number information.

IDs no longer required at commercial airports. Given that at least six hijackers used state-issued IDs or drivers' licenses at airport check-in counters on the morning of 9/11, REAL ID requires passengers to present a secure ID before boarding a commercial airplane. PASS ID eliminates this provision, allowing anyone to board a commercial aircraft whether or not he or she has a secure ID.

Eliminate information sharing among states. The 9/11 Commission also found that the 9/11 hijackers held multiple drivers' licenses and IDs from multiple states, similar to bad drivers, drug runners, counterfeiters, and others trying to circumvent the law. While REAL ID grants have been given to the states to create an information-sharing system to ensure that applicants no longer hold driver's licenses from other states, PASS ID would end that program, replacing it with a demonstration project that would likely never produce a usable system.

Eliminates all security plans. PASS ID does require public notice of security and privacy policies, but does not require security plans as mandated for compliance under REAL ID.

PASS ID would *add:*

Enhanced Driver Licenses. PASS ID does enable the Secretary of Homeland Security to certify Enhanced Driver Licenses, now produced by four states (Washington, Michigan, New York, and Vermont) as valid for land border crossing under the Western Hemisphere Travel Initiative, as compliant with REAL ID. EDLs are issued only to U.S. citizens on a volunteer basis, but are considered a strong success and somewhat like a trusted-traveler card by border personnel. With EDLs in PASS ID, EDL states would have access to REAL ID monies. This designation could spur Arizona and Texas, which both are close to EDL implementation, to become operational and issue EDLs to interested citizens.

No skimming of MRZ zones. PASS ID makes illegal the knowing scanning of information in a machine-readable

zone of a driver's license or ID card, or the reselling of such information, a common practice amongst retailers who use such information today to retain information on credit card purchases or by secure facilities to maintain records of persons seeking entry.

New grants and no fees. A new grant program is created to replace the current REAL ID grant program (still holding $50 million in appropriations) that assures every state and territory will receive PASS ID monies but does not require an accounting of monies received. In addition, any state that uses the SAVE database maintained by USCIS and mandated in PASS ID for legal-status checks, or chooses to use any other federally maintained database, will gain access for free (as opposed to cost, or, in the current rules, for a fee).

New rulemaking. PASS ID requires brand new rulemaking. Prior rulemaking took three years. The draft language states DHS must produce rules within nine months, but DHS representatives have quietly admitted no regulations are possible for at least a year and a half.

Conclusion

Those actively seeking REAL ID repeal have highlighted the law as an unfair burden on states and an affront to personal privacy. PASS ID minimizes the burden on states by freezing most states' Motor Vehicle Administration issuance practices as is, a stated purpose of the bill when discussed behind closed doors. However, the introduction of PASS ID interrupts about thirty states' work n21 to aggressively meet REAL ID's first eighteen compliance benchmarks that they are to meet by January 1, 2010, as set out by REAL ID regulations. n22

When a state issues a driver's license or ID, both the state and the individual should be confident that the license is a secure, authenticated credential. The DHS issued final regulations for REAL ID in January 2008, based on thousands of comments from states and other interested parties. Many states have already made significant progress toward this end. States are working toward implementation, spending millions of dollars to improve their issuing systems; $149 million was allocated to states in 2008, and another $50 million is waiting for distribution.

PASS ID specifically repeals identity verification (ensuring people are who they say they are) and provides broad leeway to states to fulfill the new PASS ID standards with little accountability. Broader goals of REAL ID, such as enhancing national security, increasing driver safety, combating drug running, and better safeguarding against identity theft and fraud, are nearly zeroed out in PASS ID.

PASS ID Act creates an atmosphere where an applicant's identity du jour can pass muster and be issued a legitimate driver's license or ID card with a "unique symbol" indicating the issuing state has complied with federal standards. This ID would then have expanded use under the bill's definition of "official purpose," enabling access to federal national security facilities and nuclear power plants. A PASS ID could be used to board a commercial aircraft, but the bill makes clear that no ID would be required to board a plane under PASS ID. However, a PASS ID could be used in circumstances that drivers' licenses are today, such as establishing identity for employment with programs such as E-Verify.

PASS ID is not security for the nation or the consumer. It is putting the brakes on in an era when national security, identity theft, and illegal immigration are all high-priority policy issues.

Return to Text

n1 Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Public Law No. 109-13, div. B., §§ 201-207, *119 Stat. 231* (May 11, 2005). Title II is titled

Improved Security for Drivers' Licenses and Personal Identification Cards. It can be found as a note to *49 U.S.C.S. § 30301*.

n2 S. 1261, sponsored by Senators Akaka, Baucus, Carper, Leahy, Tester, and Voinovich, later joined by Senator Alexander, *available at* http://www.thomas.gov/cgi-bin/query/z?c111:S.1261:.

n3 National Commission on Terrorist Attacks Upon the United States, 9/11 and Terrorist Travel 44 (Hillsboro Press 2004).

n4 *Id.* at 43.

n5 *Id.* at 44.

n6 *Id.* at 221 n.202.

n7 *Id.* at 44.

n8 National Commission on Terrorist Attacks Upon the United States, *Chapter 7, The Attack Looms, in* The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (2004).

n9 National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States 387, 390 (W.W. Norton & Co. 2004).

n10 Janice Kephart, NJ's Legal Presence Requirements Made a Difference in the Fort Dix Plot, http://www.cis.org/kephart/fortdix (Dec. 30, 2008).

n11 For use by states of SAVE, see Janice Kephart, Secretary Chertoff's Stocking Stuffer: States Get Infusion of Secure ID Monies, http://cis.org/kephart/chertoffsstockingstuffer (Dec. 19, 2008). For Maryland's legislation, see Press Release, Maryland Department of Transportation Motor Vehicle Administration, New Law Requires Proof of Legal Presence to Receive Maryland Driver's License or ID Card; Requirement Begins June 1, 2009 (Apr. 16, 2009), *available at* http://www.marylandmva.com/AboutMVA/PRESS/090416.htm (last visited June 26, 2009).

n12 American Association of Motor Vehicle Administrators, AAMVA DL/ID Security Framework (Feb. 2004), *available at* http://www.aamva.org/aamvaDocumentDisplay.aspx?id=[25BBD457-FC4F-4852-A392-B91046252194] (last visited June 26, 2009).

n13 *Id.* at 8.

n14 *73 Fed. Reg. 5272* (Jan. 29, 2008) (codified at 6 C.F.R. pt. 37); Janice L. Kephart, REAL ID Final Rules: a Summary (Feb. 2008), http://www.911securitysolutions.com/docs/REALIDFinalRules.pdf (last visited June 26, 2009).

n15 6 C.F.R. §37.15(a).

n16 6 C.F.R. §37.41(b)(2)(i).

n17 *Id.*

n18 *18 U.S.C. § 2721.*

n19 6 C.F.R. §37.45(b)(2). E-Verify is discussed extensively in Ann Allott, Daniel Kowalski & Camille Griffin, Immigration Enforcement: I-9 Compliance Handbook §5.04 (2009).

n20 PASS ID does maintain the lawful-presence checks of REAL ID, which is an important standard for drivers'-license security. Maryland recently began checking lawful presence, after finding that allowing illegal immigrants to obtain Maryland driver's licenses had made the state a magnet for fraud, crime, and bad drivers. Governor O'Malley, a co-chair of the National Governors Association's Homeland Security Committee, signed a bill to comply with REAL ID on May 8, 2009. Laura Smitherman, *O'Malley Signs Contentious New Laws*, Baltimore Sun, May 8, 2009, at 3A, *available at* http://www.baltimoresun.com/news/local/politics/bal-md.bills08may08,0,7190848.story (last visited June 26, 2009); *see also* Posting of Andy Green, O'Malley's Position on Real ID, *Baltimore Sun* Maryland Politics blog, http://weblogs.baltimoresun.com/news/local/politics/2009/03/omalleys_position_on_real_id.html (Mar. 31, 2009, 2:39 p.m.) (last visited June 26, 2009).

n21 Janice L. Kephart & Jena Baker McNeil, The PASS ID Act: Rolling Back Security Standards for Driver's Licenses (Heritage Foundation Backgrounder No. 2288, June 23, 2009), *available at* http://www.heritage.org/Research/HomelandSecurity/bg2288.cfm (last visited June 29, 2009).

n22 Janice L. Kephart, REAL ID Final Rules: a Summary (Feb. 2008), http://www.911securitysolutions.com/docs/REALIDFinalRules.pdf (last visited June 26, 2009).

RELATED LINKS: For more on the REAL ID regulations, see Joe Whitley's and Brian Frey, Joe Whitley & Brian D. Frey, DHS's Final Regulations Implementing Title II of the REAL ID Act of 2005,
- 2008 Emerging Issues 2214.

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

ABOUT THE AUTHOR(S):
Janice L. Kephart is a former counsel to the September 11 Commission and is National Security Policy Director for the Center for Immigration Studies.

Amanda Frost on Government Use of the State Secrets Privilege

2008 Emerging Issues 3062

Amanda Frost on Government Use of the State Secrets Privilege

By Amanda Frost

November 30, 2008

SUMMARY: Professor Amanda Frost discusses the governments use of the state secrets privilege as a ground for excluding evidence, or dismissing claims, that it argues could jeopardize national security. Professor Frost reviews the case law, theories like the "mosaic theory" supporting the privilege, and alternatives to exclusion or dismissal.

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

ARTICLE: The state secrets privilege is an evidentiary privilege that excludes from discovery in civil litigation documents whose production could harm national security. Some courts have concluded that the privilege also requires the dismissal of claims or even entire lawsuits when litigation of such claims would jeopardize national security.

(1) Origins of the Privilege

A. *United States v. Reynolds*

The state secrets privilege was first explicitly recognized by the Supreme Court in its 1953 decision in *United States v. Reynolds,* n1 which remains the only case in which the Supreme Court discussed the privilege at any length. *Reynolds* involved a claim for damages against the federal government brought by the widows of three civilians killed in the crash of a B-29 aircraft. During discovery, the plaintiffs sought production of the U.S. Air Forces official accident investigation reports and statements made by three surviving crew members. The United States objected, claiming that the heads of executive departments had constitutional authority to withhold documents from judicial review whenever they deemed it in the public interest to do so. n2 The Supreme Court rejected this broad proposition[], n3 but explicitly noted for the first time the existence of a privilege to protect military and state secrets.

The *Reynold*s Court ultimately accepted the governments representations about the classified nature of the evidence being sought and refused to require disclosure. The Court remanded the case so that litigation could proceed, declaring that it should be possible for respondents to adduce essential facts as to causation without resort to material touching upon military secrets. n4 The parties eventually settled the case.

The accident report at issue in *Reynolds* was declassified many years later and, according to leading experts, revealed . . . serious negligence by the government, but contained nothing that could be called state secrets. n5 For that

reason, some commentators have urged courts to carefully scrutinize the the materials in dispute to ensure the privilege applies, rather than to simply accept executive assertions of the privilege. n6

B. *Totten v. United States*

Although *Reynolds* is the first explicit recognition of a state secrets privilege, it was not the first time the government claimed that litigation threatened national security. The 1875 decision in *Totten v. United States* is one of the Courts earliest cases addressing the issue, and is also one of only two cases in which the Court ordered that the case be dismissed because its very subject matter concerned secret evidence. n7 *Totten* involved a contract dispute between a Union spy and President Abraham Lincoln. The contract, which the parties entered into in July 1861, provided that the spy was to travel behind rebel lines and transmit information about the Confederate Army in return for payment of $ 200 per month. The spy performed the tasks agreed upon, but was reimbursed only for his expenses. The Supreme Court concluded that although President Lincoln had the authority to enter into the contract, no court could enforce it. The Court then stated: [A]s a general principle . . . public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated. n8 Accordingly, the Court dismissed the case.

Totten was recently reaffirmed by the Supreme Court in *Tenet v. Doe*, a case in which two former spies claimed that the government had reneged on its agreement to provide lifetime support for them in the United States in return for espionage services in their native country. n9 Their complaint alleged that the government had violated their equal protection and due process rights by refusing to abide by the terms of their original agreement. The Supreme Court held that the so-called *Totten* bar precludes judicial review of any claim based on a covert agreement to engage in espionage for the United States. n10

(2) Implementing the State Secrets Privilege

Below is a discussion of how the state secrets privilege is implemented in litigation. Some aspects of the privilege remain unclear. As one academic commentator has noted, the nature and scope of the state secrets privilege remain the subject of considerable uncertainty. n11 For example, there is no consensus over the degree of deference given to executive branch assertions of the privilege, the standard for determining whether the privilege applies, or the consequences of an assertion of the privilege.

A. The U.S. Government Alone Controls Assertion of the Privilege

Only the U.S. government can assert the state secrets privilege, which can neither be claimed nor waived by a private party. n12 The privilege can nonetheless arise in litigation solely between private parties if the government intervenes and asserts the privilege to prevent discovery of information held by a private party that the government believes is protected by the state secrets privilege. n13

The privilege can be asserted only by the head of an executive branch agency with control over the secret information at issue, and only after that person has filed an affidavit demonstrating that he or she has personally reviewed the information and determined that it qualifies as state secrets. n14

B. Judicial Review of Executive Assertions of the Privilege.

Reynolds made clear that the judicial branch must ultimately decide whether the evidence is admissible, stating that [j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers. n15 A judge can conduct an *in camera* review of the evidence, although that is not necessary when the context in which the evidence is raised clearly demonstrates the need for the privilege, as the Court concluded was the case in *Reynolds.* n16

Reynolds stated that the privilege applies when a court determines that there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, shall not be divulged. n17 But

the Court stated that its scrutiny of a claim of privilege would be calibrated to the necessity of the evidence to the case: Where there is a strong showing of necessity, the claim of privilege should not be lightly accepted, but even the most compelling necessity cannot overcome the claim of privilege if the court is ultimately satisfied that military secrets are at stake. n18

Although *Reynolds* made clear that courts, and not executive branch officials, are to determine whether the privilege applies, many lower courts are reluctant to second-guess executive claims regarding the harm that would result to the nations security were it forced to disclose information sought in discovery. For example, in granting the governments motion to dismiss Maher Arars lawsuit challenging his rendition by the U.S. government, the district court observed that courts must [] bear in mind the Executive Branchs preeminent authority over military and diplomatic matters and its greater expertise relative to the judicial branch in predicting the effect of a particular disclosure on national security. n19 The Fourth Circuit affirmed the district court, again citing the need for deference to the executive in this area. n20

However, a few judges have refused to defer to executive claims of privilege. For example, District Judge Vaughn Walker commented that he viewed the state secrets privilege as limited, at least in part, by the role of the judiciary in the constitutional structure:

[I]t is important to note that even the state secrets privilege has its limits. While the court recognizes and respects the executives constitutional duty to protect the nation from threats, the court also takes seriously its constitutional duty to adjudicate the disputes that come before it. . . . To defer to a blanket assertion of secrecy here would be to abdicate that duty. . . . n21

C. The Effect of the State Secrets Privilege.

Extrapolating from the brief description of the state secrets privilege in *Reynolds*, lower courts have concluded that it can affect litigation in a number of ways.

First, it is clear from the result in *Reynolds* that the privilege can bar evidence from admission in litigation. The plaintiffs case will then go forward without the excluded evidence, and will be dismissed only if the plaintiff is unable to prove the prima facie elements of the claim without it. n22

Second, lower courts have concluded that if the privilege deprives the defendant of information that would provide a valid defense, then the court may grant summary judgment for the defendant. n23

Third, some courts have held that if the very subject matter of the action is a state secret, then the court should dismiss the plaintiffs action based solely on the invocation of the state secrets privilege. n24 However, the Supreme Court has taken such drastic action only in the very narrow category of cases involving covert espionage agreements, such as *Totten v. United States* and *Tenet v. Doe*, described above. Thus, it is not clear that the Court ever intended the evidentiary privilege it recognized in *Reynolds* to serve as a jurisdictional bar to civil litigation.

D. Segregability and the Mosaic Theory

Even when a court finds that a document relevant to the litigation contains state secrets, it should not order the exclusion of the entire document. If possible, the government should produce the document after redacting the sensitive information. n25

However, some courts have refused to require the disclosure of even seemingly innocuous information in such documents under the so-called mosaic theory. The D.C. Circuit first articulated this concern, warning that thousands of bits and pieces of seemingly innocuous information can be analyzed and fitted into place to reveal with startling clarity how the unseen whole must operate. n26 The Ninth Circuit subsequently held that if seemingly innocuous information is part of a classified mosaic, the state secrets privilege may be invoked to bar its disclosure and the court cannot order

the government to disentangle this information from other classified information. n27

The mosaic theory is problematic, however, since taken to its logical extreme it potentially results in excluding vast amounts of information that independently would not qualify for the state secrets privilege. Perhaps for that reason, the mosaic theory has been infrequently cited in judicial opinions discussing the privilege.

E. Alternatives to Dismissing Litigation or Excluding Evidence that Qualifies for the State Secrets Privilege.

As some commentators have noted, dismissing cases challenging the legality of government conduct on state secrets grounds raises serious separation of powers concerns. n28 The federal courts play an essential role in checking the power of the executive, thereby preventing the tyranny that results from the accumulation of all powers legislative, executive and judiciary in the same hands. n29 Accordingly, the Supreme Court has repeatedly asserted its power to review constitutional claims, despite executive and legislative attempts to strip courts of jurisdiction, observing that serious constitutional questions [] would arise if a plaintiff were denied any judicial forum for a colorable constitutional claim. n30 Unchecked assertion of the state secrets privilege is constitutionally problematic because it ousts the courts from safeguarding individual rights against executive overreaching.

For that reason, plaintiffs should urge courts to consider alternative methods of protecting state secrets from disclosure that would nonetheless allow litigation to go forward. Courts are well equipped to apply safeguards and protective procedures that would allow litigation to proceed without jeopardizing national security. Indeed, courts have done so on a regular basis for decades.

For example, in cases concerning requests for classified documents brought under the Freedom of Information Act (FOIA), the government has long been required to generate an index describing each document withheld and explaining the basis for the executives claim that its disclosure would harm national security. n31 This procedure allows both the court and the opposing party to determine which documents are truly relevant and to challenge the basis for the executives claim that the documents must remain secret. In addition, courts regularly mandate that the United States segregate any nonclassified material from classified documents to provide the FOIA requester with as much information as possible. n32

The Classified Information Procedures Act (CIPA) provides another model for courts seeking to balance the governments need for secrecy against a litigants right to access to courts. Under CIPA, the court responds to a defense request for classified documents by first determining whether the evidence sought is relevant and material. If so, the burden shifts to the government to show that the information contains sensitive information about national security that cannot be publicly disclosed. n33 Even if the government satisfies its burden, the information is not completely withheld from the defendant. Rather, the court decides whether a modification or substitute for the evidence is possible. CIPA requires the government to produce redacted versions of documents, submit a summary of the information in the classified documents, or substitute a statement admitting relevant facts that the classified documents would prove. n34 Similar procedures could be followed in civil cases. n35

Litigants seeking to proceed with litigation despite the governments assertion of the state secrets privilege should request that the court apply one of the protective measures used in FOIA and CIPA litigation to allow the litigation to proceed despite the claim of privilege.

F. Common Law Privilege or a Constitutional Privilege?

Most courts describe the state secrets privilege as a common law evidentiary privilege, and not a constitutionally derived privilege. n36 Although the Supreme Court did not explicitly address that question in *United States v. Reynolds*, its discussion of the privilege suggested it was grounded in common law.

Nonetheless, some government officials and a few courts have suggested that the state secrets privilege is rooted in the Constitution, n37 citing dicta from *United States v. Nixon* to support that conclusion. *Nixon* did not concern the

state secrets privilege, but instead the presidents claim that the executive privilege permitted him to withhold from the Watergate Special Prosecutors tapes and transcripts of conversations between the president and his advisors. n38 The Court concluded that the executive privilege did not protect the materials, and ordered their disclosure. In the course of reaching that conclusion, the Court noted that the information at issue did not concern military or diplomatic secrets, which it described as areas of Art. II duties courts have traditionally shown the utmost deference. n39

The question whether the state secrets privilege is grounded in common law or the Constitution is not significant for most litigants, however. Even if the privilege is constitutionally mandated, it nonetheless is not absolute and is subject to judicial review, as is the case with the constitutionally based executive privilege discussed in *Nixon.* n40

Return to Text

n1 *345 U.S. 1, 6-7 (1953).* Although this was the first case in which the Court explicitly recognized the privilege, the Court stated that the privilege was well established, stretching back at least to the 1807 trial of Aaron Burr for treason. *Id. at 9.* For an in-depth discussion of the *Reynolds* litigation, see Louis Fisher, In the Name of National Security: Unchecked Presidential Power and the *Reynolds* Case 29-118 (2006).

n2 *Reynolds, 345 U.S. at 6* & n.9.

n3 *Id.*

n4 *Id. at 11.*

n5 Fisher, *supra* note 1, at xi; *see also* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation, 75 Geo. Wash. L. Rev. 1249, 1288 (2007)* (It is now known that the investigative report at issue in that case did not actually contain information about the classified equipment that had been aboard the doomed flight.).

n6 *See id. at 1288.*

n7 *See Reynolds, 345 U.S. at 7 n.11* (citing *Totten v. United States, 92 U.S. 105, 107 (1875)).*

n8 *Totten, 92 U.S. at 107.*

n9 *544 U.S. 1 (2005).*

n10 *See id. at 3.*

n11 Chesney, *supra* note 5, at 1270.

n12 *Tenet* at 7.

n13 *See, e.g.*, Hepting v. AT& *T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006)* (U.S. government intervened in litigation challenging AT&Ts alleged warrantless wiretapping of plaintiffs communications and filed a motion to dismiss on state secrets grounds), *remanded, 539 F.3d 1157 (9th Cir. 2008).*

n14 *Reynolds, 345 U.S. at 7-8* (There must be a formal claim of privilege, lodged by the head of the department which has control over the matter, after actual personal consideration by that officer.).

n15 *Id. at 8.*

n16 *Id. at 10.*

n17 *Id.*

n18 *Id. at 11.*

n19 *El-Masri v. Tenet, 437 F. Supp. 2d 530, 536 (E.D. Va. 2006), affd, El-Masri v. United States, 479 F.3d 296 (4th Cir. 2007), cert. denied, 169 L. Ed. 2d 258, 128 S. Ct. 373 (2007).*

n20 *El-Masri, 479 F.3d at 305.*

n21 *Hepting, 439 F. Supp. 2d at 995* (internal citations omitted).

n22 *See, e.g., Ellsberg v. Mitchell, 709 F.2d 51, 65 (D.C. Cir. 1983)* (remanding case to determine whether plaintiffs could prove *prima facie* case without privileged information).

n23 *See, e.g., Bareford v. General Dynamics Corp., 973 F.2d 1138, 1141 (5th Cir. 1992); Molerio v. FBI, 749 F.2d 815, 825 (D.C. Cir. 1984).*

n24 *Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998)* (quoting *Reynolds, 345 U.S. at 11 n.26).*

n25 *Ellsberg* at 57 ([W]henever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.).

n26 *Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978).*

n27 *Kasza, 133 F.3d at 1166.*

n28 *See, e.g.*, Fisher, *supra* note 1, at 262; Amanda Frost, *The State Secrets Privilege and Separation of Powers, 75 Fordham L. Rev. 1931 (2007);* William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 Pol. Sci. Q. 85, 90 (2005).

n29 The Federalist No. 47, at 324 (James Madison) (J. Cooke ed., 1961).

n30 *Webster v. Doe, 486 U.S. 592, 603 (1988)* (citing *Bowen v. Michigan Acad. of Family Physicians, 476 U.S. 667, 681 n.12 (1986)).*

n31 *See Vaughn v. Rosen, 484 F.2d 820 (D.C. Cir. 1973).*

n32 *See, e.g., Schiller v. NLRB, 964 F.2d 1205, 1209 (D.C. Cir. 1992).* As discussed above, courts have similarly required the government to do the same when asserting the state secrets privilege. *See Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983)* ([W]henever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter.).

n33 *See United States v. Yunis, 867 F.2d 617, 622 (D.C. Cir. 1989).*

n34 *18 U.S.C. App. § 4.*

n35 Legislation is pending in Congress that would regulate use of the state secrets privilege through procedures akin to those used in CIPA. *See* The State Secrets Protection Act of 2008, S. 2533, 110th Cong.; The State Secrets Protection Act of 2008, H.R. 6507, 110th Cong.

n36 *See, e.g., United States v. Aref, 533 F.3d 721, 728 (2d Cir. 2008); Al-Haramain Islamic Foundation v. Bush, 507 F.3d 1190, 1196 (9th Cir. 2007).*

n37 Letter from Michael Mukasey, U.S. Atty Gen., to Sen. Patrick Leahy (Mar. 31, 2008), *available at* http://www.usdoj.gov/ola/views-letters/110-2/03-31-08-ag-ltr-re-s2533-state-secrets.pdf; *see also El-Masri v. United States, 479 F.3d 296, 303-04 (4th Cir. 2007)* (noting that the privilege was developed at common law, but stating that it also has a firm foundation in the Constitution). An evaluation of Attorney General Mukaseys letter to Senator Leahy, in the form of a letter from Louis Fisher of the Library of Congress to Senator Edward Kennedy, LL File No. 2008-000846 (Apr. 2, 2008), is *available at* http://www.fas.org/sgp/jud/statesec/fisher040208.pdf

n38 *United States v. Nixon, 418 U.S. 683 (1974).*

n39 *Id. at 710.*

n40 *Nixon, 418 U.S. at 707* & 711 (describing the privilege as constitutionally based, but nonetheless concluding that it is not absolute, and must give way in light of the legitimate needs of the judicial process).

RELATED LINKS: Steve C. Posner,
- Privacy Law and the USA PATRIOT Act § 4.44.

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

ABOUT THE AUTHOR(S):

Amanda Frost is an Associate Professor of Law at American Universitys Washington College of Law. Before joining WCL in 2004, she was an attorney with Public Citizen. She has consulted for the Open Society Foundation and USAID. In 2001, she was awarded a Fulbright Scholarship. After graduating from Harvard College and Harvard Law School, she clerked for Judge A. Raymond Randolph of the U.S. Court of Appeals for the D.C. Circuit. She specializes in federal courts/federal jurisdiction, civil procedure, statutory interpretation, and government transparency. More information is at http://www.wcl.american.edu/faculty/frost/.

Lawrence O. Gostin on Biosecurity Policy: Are We Safer Today?

2008 Emerging Issues 2918

Lawrence O. Gostin on Biosecurity Policy: Are We Safer Today?

By Lawrence O. Gostin

September 16, 2008

SUMMARY: World-acclaimed authority Lawrence O. Gostin analyzes biosecurity policy since 9/11. He begins with the question: Are we safer now? Then comes a review of biosecurity legislation, followed by discussion of planning to deal with specific diseases and the problems with such an approach, and then an explanation of what the right approach is. He concludes by covering the Model State Emergency Health Powers Act and related civil liberties questions.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: In the wake of the trauma of September 11, 2001, the United States and the rest of the world have feared, and prepared for, the next mass disaster, whether biological, nuclear, chemical, or natural (such as a hurricane, tsunami, or earthquake). n1 Biosecurity policy has lurched from one scare to the next, ranging from anthrax, smallpox, and SARS to avian influenza. Even small clusters of disease caused by a homegrown terrorist can produce enormous anxiety, as the recent debates over the identity of the anthrax suspect Bruce Ivins amply demonstrate. In response, the government has gone to war in Iraq and Afghanistan, poured billions of dollars into biosecurity preparedness, and entirely reorganized public health and emergency services through the Department of Homeland Security (DHS). But, with all the planning and resources, a single question remains--are we safer today than we were before the attacks on the World Trade Center and the subsequent anthrax outbreaks?

Are We Safer?

Since 9/11 and the anthrax attacks, a substantial federal investment totaling nearly $50 billion has been allocated to increase our nations ability to prepare for, and respond to, public health emergencies. Congress and the administration have launched a myriad of biosecurity measures. Despite government claims that we are much safer, it is unclear whether these policies and investments have left the nation better prepared for the next bioterrorist attack, epidemic, or any other large-scale public health emergency. n2 This situation is not due to a shortage of biosecurity measures, but to vague goals, weak accountability, and the wrong priorities. Rather than focus on remote risks that happen to garner public attention, it would be far more cost effective to build health system capacity--for research (vaccines and pharmaceuticals), public health (laboratories, surveillance, and response), and health care (clinics, hospitals, and medical equipment).

This commentary first reviews biosecurity legislation and disease-specific plans that the President has trumpeted as

models of success, but that have been mostly ineffective, and in some cases costly failures. It then describes what real reform would entail, with the potential to make the nation far safer.

Biosecurity Legislation

Among the myriad of initiatives to improve public health emergency preparedness, perhaps the most highly touted are BioShield and the Pandemic and All-Hazards Preparedness Act. These statutes improve governance in a public health emergency and incentivize industry to develop medical countermeasures, but have serious deficiencies.

Project BioShield; Vaccine Development

The biotechnology industry has not systematically developed countermeasures for emerging infectious diseases and bioterror agents because the market is speculative. As a result, industry has focused on products of commercial value. According to the Institute of Medicine, vaccine development has been poorly organized, planned, and funded, putting the nation at risk. n3 To encourage companies to develop new biodefense countermeasures, Congress enacted Project BioShield Act of 2004, n4 which establishes a Special Reserve Fund of $5.6 billion over ten years to purchase medical countermeasures against a broad array of chemical, biological, radiological, and nuclear agents. BioShield also authorizes the Food and Drug Administration (FDA) to permit rapid distribution of promising yet unapproved and unlicensed new drugs and antidotes in emergencies.

Project BioShield has not encouraged industry to develop vaccines, as shown by the limited number of countermeasures it has procured for the stockpile. The DHS has thus far authorized special reserve funds for only four countermeasures (anthrax, smallpox, botulinum toxin, and radiological/nuclear devices), and has awarded few contracts. Commentators attribute this lack of success to several factors. n5 First, BioShield is a late-stage procurement program, so that industry bears financial risk for early research and development. Small biotech companies, in particular, cannot afford the considerable start-up costs. Second, funding levels were insufficient to entice larger pharmaceutical companies because selling a product for procurement to the U.S. stockpile was not as lucrative as popular commercial products. Third, if countermeasures fail in development, or if the government decides not to procure the product after development, biopharmaceutical companies would sustain significant loses. And in several cases federal agencies have canceled or delayed requests for proposals or industry contracts. Finally, the industry has expressed concerns about liability associated with developing untested countermeasures. Beyond all of this, BioShield is restricted to intentional acts of terror and not naturally occurring infectious diseases, which means it has little utility in the event of a major naturally occurring epidemic.

PAHPA: Pandemic Preparedness

The Pandemic and All-Hazards Preparedness Act (PAHPA) was enacted in 2006 to improve the organization, direction, and utility of preparedness efforts. n6 PAHPA centralizes federal responsibilities, requires state-based accountability, proposes new national surveillance methods, addresses surge capacity, and improves BioShield. PAHPA aspires to answer the pivotal question of who is in charge by placing the Department of Health and Human Services (DHHS) as the lead agency for federal public health and medical response[s] to public health emergencies covered by the National Response Plan, which otherwise vested most emergency management functions in the DHS. n7 The problem is that states have the historic and primary constitutional police powers to safeguard the publics health. n8 PAHPA acknowledges the importance of interjurisdictional coordination, but does not specify how federal entities should align with tribal, state, and local governments. The Act does little to instill confidence that the leadership and coordination so painfully absent during Hurricane Katrina will change in the face of a new disaster.

Meeting surge capacity during catastrophic events is also a key priority. Rather than ensuring an adequate number of well trained health professionals and critical medical equipment, PAHPA focuses on federal oversight of volunteers through the Emergency System for Advance Registration of Volunteer Health Professionals (ESAR-VHP) and Medical Reserve Corps (MRC). PAHPA coordinates qualified volunteers, but does not motivate them or the entities that send or

host them by reducing the fear of civil recourse. PAHPA represents a missed opportunity to appoint emergency volunteers as federal employees so that they could be protected from liability like members of the U.S. Public Health Service Commissioned Corps.

Finally, and importantly, PAHPA promises rapid development of biological interventions, attempting to rectify the entrenched problems in BioShield. The Act establishes a new Biomedical Advanced Research and Development Authority (BARDA) within the DHHS charged with fostering collaboration, supporting research, encouraging innovation, and offering technical guidance. PAPHA authorizes $1 billion through the Biodefense Medical Countermeasure Development Fund, and grants the DHHS authority to support advanced-stage research and development. Yet, PAHPA still does not recognize practical market-based realities or overcome political apathy. It fails to authorize sufficient funding to create strong incentives, and Congress has allocated only a small percentage of the funds that were authorized.

Disease-Specific Plans: The Wrong Approach and Flawed Implementation

The government has devoted enormous energy to and resources on a few diseases that have captured public and political attention, but pose relatively remote risks. In this sense, policy has been highly reactive, lurching from one disease to the next, rather than taking an all-hazards approach. In response to a handful of anthrax cases in 2001, the government compelled vaccination in the military. The President wrongly perceived that Saddam Hussein had biological weapons, so he launched a mass smallpox vaccination campaign the following year. More recently, the federal government has expended vast resources on pandemic influenza, which is a serious threat, but has thus far been confined almost exclusively to avian populations. The problem in each case was not simply that the government had the wrong priorities, but that it mismanaged the response.

Anthrax: Ineffective Vaccine and Flawed Criminal Investigation

Until the FDA approved the anthrax vaccine absorbed (AVA) in December 2003, there was no approved anthrax vaccine. Nonetheless, in 1998 the Department of Defense (DoD) established the Anthrax Vaccine Immunization Program (AVIP), designed to achieve total force protection against anthrax by 2004. The military is concerned about battlefield safety, but the AVIP remains highly controversial. The evidence for the safety and effectiveness of the anthrax vaccine is equivocal. Members of the armed forces are concerned about possible adverse effects in the short and long term, and they question the DoDs decision to compel soldiers to be vaccinated against their will. In 2003, members of the armed forces successfully challenged the AVIP in *Doe v. Rumsfeld*. n9 Days after the court halted the program, the FDA published a final rule categorizing the vaccine as safe and effective for use against inhalation anthrax. n10 In doing so, however, the FDA violated its own rules requiring time for meaningful public comment, so the judiciary halted the program again in October 2004. n11 For the next two years, the program proceeded under a voluntary protocol and participation rates did not exceed 50%. After the FDA issued a proper formal rule finding the vaccine safe and effective, the DoD announced on October 15, 2006, that it would resume mandatory anthrax vaccinations.

As this poorly planned military vaccination program unfolded, there has been continuing concern about the effectiveness of the anthrax vaccine. The AVA does not protect individuals from spore germination, infection, and/or bacteremia. Moreover, protective immunity must be generated via a lengthy injection schedule and maintained by a yearly booster. n12 Yet, despite intense efforts, little progress has been made in finding a more effective vaccine. n13

In addition to anthrax vaccine improvement, the other major government priority was to identify and successfully prosecute the individual(s) who sent highly refined anthrax spores through the mail in 2001. Some seven years later, after appearing to implicate the wrong person, the Federal Bureau of Investigation (FBI) laid out its case against Bruce Ivins, a microbiologist at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) in Fort Detrick, Maryland. Mr. Ivins committed suicide prior to formal charges being filed, amidst lingering doubts. I don't think we're ever going to put the suspicions to bed, said an FBI spokesman. There's always going to be a spore on a grassy knoll. n14

The fact that a U.S. Army laboratory specialist possibly perpetrated the most serious bioterrorist attack on American soil has worried commentators. n15 The number of laboratories working with highly dangerous, top security pathogens is exponentially greater today than it was in 2001. That leaves the potential for laboratory employees to exploit their positions, either by engaging in acts of terror themselves or helping others secure highly pathogenic strains.

The Smallpox Vaccine Campaign: Mass Immunization for an Eradicated Disease

If anything the smallpox vaccination campaign launched by President Bush on December 13, 2002, was even more speculative and flawed than the response to anthrax. More than twenty years earlier the World Health Organization certified the global eradication of smallpox, and the last vaccinations in the United States were given in the 1970s.

The national smallpox vaccination plan represented an extraordinary policy decision--mass vaccination against a disease that did not exist with a vaccine that had well documented risks. The plan had several phases: immediate and mandatory vaccination of half a million military personnel who are or may be deployed in high threat areas; voluntary vaccination of up to 500,000 health care workers and smallpox response teams within thirty days; vaccination of up to ten million health care personnel and other first responders, such as firefighters and police; and vaccination with a new, not-yet-approved vaccine to members of the public who insist on access.

The military smallpox vaccination program went essentially as planned; in less than six months the DoD administered 450,293 smallpox vaccinations. The plan to vaccinate up to 500,000 civilian health care workers who would be responsible to vaccinate the public in the event of a smallpox attack, however, faltered badly, and was officially paused in June 2003, with a response rate of less than 10% of eligible physicians and nurses. The campaign, if successfully implemented, would have subjected healthy volunteers to the risk of adverse effects, ranging from mild and self-limited to severe and life-threatening. Vaccinated individuals also could transmit vaccinia to close contacts. The programs justification was the risk of intentional release of smallpox virus, but the White House did not disclose evidence that the virus existed outside the two known repositories. The CDCs vaccine advisory committee said the risk was low and indeterminate. n16 Never before had a vaccination program been undertaken where there was no natural hazard but only the hypothetical threat posed by the possibility of a terrorist attack.

The national smallpox vaccination campaign was the subject of intense criticism. The Institute of Medicines principal findings were that White House had failed to communicate the policys rationale and curtailed the CDC from communicating with key constituencies. n17 The American Public Health Association stated that the CDCs implementation plan did not provide adequate resources, including costs derived from monitoring adverse events, treating complications, and training personnel. n18 The vaccine industry and hospitals that administered vaccinations sought, and received, tort immunity in 2002. Health care workers requested compensation for injuries resulting from smallpox vaccination, but Congress did not enact a plan until April 2003, after highly publicized cases of serious adverse events. In the end, the government could not secure the needed buy-in and participation of public health and health care professionals. The unifying theme was a lack of planning and collaboration with major stakeholders that resulted in a loss in trust in government, which ultimately led to the plans failure.

The national smallpox vaccination program offers a poignant case study at the intersection of public health and national security. The order for vaccinations came from the highest level--the President of the United States. It began with intense media coverage of smallpox in the aftermath of the trauma of September 11, and continued with the build-up to the war in Iraq. Public health and health care professionals remained deeply skeptical and dodged in the face of a Presidents call to action. In many ways, the breakdown in trust between national security and public health was sad and remarkable--a lesson that, if not learned well, could harm national interests in a time of crisis.

Highly Pathogenic Influenza: A Future Pandemic?

Highly pathogenic Influenza A (H5N1) has captured the close attention of policy makers who regard pandemic influenza as a national security threat. The virus is endemic in avian populations in Southeast Asia, with serious

outbreaks now in Africa, Europe, and the Middle East. International trade, travel, and migratory birds will likely bring the infection to other continents. The economic consequences are severe, with millions of birds culled or dead from infection, and bans placed on poultry imports.

Although the H5N1 virus is highly contagious among birds, it is rare in humans due to a significant species barrier. A few cases of human-to-human transmission have occurred, principally involving intimate contact, but transmission has not continued beyond one person. The virus appears highly pathogenic with a reported death rate exceeding 50%.

Although the prevalence is currently very low (and pales in comparison to pandemics of HIV, malaria, and tuberculosis), health officials express concern about the potential for pandemic spread. Historically, the world has experienced three or four influenza pandemics per century. The 20th century witnessed the Spanish flu (1918, H1N1, 20-50 million deaths), Asian flu (1957, H2N2, 1-2 million deaths), Hong Kong flu (1968, H3N2, 700,000 deaths), and Swine flu (1976, H1N1, no pandemic). Through adaptive mutation or viral reassortment, the virus could become highly transmissible among humans. Recent evidence that the 1918 pandemic was caused by an avian influenza virus lends credence to the theory that current outbreaks have pandemic potential. Extrapolating from the 1918 pandemic, modeling studies indicate that, in the absence of intervention, half a million to a million Americans could die, with tens of millions of deaths globally.

The United States n19 and the WHO n20 issued strategic plans to prevent and control influenza in 2005/06. Therapeutic countermeasures (e.g., vaccines and antiviral medications) and public health interventions (e.g., infection control, social separation, and quarantine) form the two principal strategies for prevention and response. Vaccination and, to a lesser extent, antiviral medication (oseltamivir [Tamiflu] or zanamivir [Relenza]) are the most important interventions for reducing morbidity and mortality associated with influenza.

Despite the promise of medical countermeasures, there is a chronic mismatch of public health needs and private control of production. Vaccine production has been unreliable even for seasonal influenza, which is the leading cause of vaccine-preventable mortality; only a fraction of the recommended population is vaccinated each year. For example, the United States lost half its supply in 2004/05 when the United Kingdom withdrew Chiron Corporations license due to bacterial contamination. The best way to ensure pandemic preparedness is to increase the baseline for seasonal countermeasures.

Public/private strategies, rather than private markets, are most likely to ensure stable, economically viable vaccines to meet potentially massive public needs. As alluded to above, market forces create disincentives that inhibit vaccine development: high investment costs, limited or variable markets, and regulatory compliance. Vaccine manufacturers are leaving the industry, creating the risk of severe shortages. In 1967, twenty-six companies were licensed for vaccines in the U.S. market, but less than half as many today; only four companies supply influenza vaccine, with only two manufacturing domestically--MedImmune (FluMist only) and Sanofi Pasteur. n21

The White House strategic plan devotes a great deal of resources to pandemic influenza. Although the threat is real, it is not certain whether the money is well spent. First, the expenditure is for a single disease threat that may or may not materialize. The vast majority of proposed expenditures in the $6.7 billion federal influenza plan is devoted to medical countermeasures: $4.7 billion for cell-based vaccine technology and stockpiling experimental vaccine, and $1.4 billion for antiviral medicines. Yet, medical countermeasures are unlikely to impede pandemic spread: Experimental H5N1 vaccines may not be effective against a novel human subtype, neuraminidase inhibitors may become resistant, and medical countermeasures will be extremely scarce. Even if all of these problems could be solved, how would it be possible to get the vaccine and antiviral medications to people? The vaccine might have to be administered in two separate doses, and the antivirals need to be administered within days of the onset of symptoms. It would not be prudent to have people leave their homes, as they might infect one another, and there are no viable plans to get the countermeasures to people in their homes in a timely manner.

This leaves conventional public health measures such as surveillance, personal hygiene, hospital infection control,

decreased social mixing/increased social distance (e.g., school and workplace closures), and isolation and quarantine. n22 Thus, the key question is: Which measure, or combination of measures, works best at each stage of the pandemic? Multiple, targeted approaches are likely to be most effective, but can have deep adverse consequences for the economy and civil liberties.

Real Reform: What Would Make the Public Healthier and Safer?

The considerable influx of funding and attention to public health emergency preparedness has undoubtedly improved safety, especially if one of the specific threats that the government has placed its bet on materializes, such as anthrax, smallpox, or Influenza A (H5N1). The time and resources, however, could be spent far more cost-effectively by focusing on building capacity for a broad range of health threats, whether naturally occurring or deliberately inflicted. n23

Real reform would have the following elements: (1) build capacity in the health system (public health and health care) to meet everyday health needs of the population; (2) ensure surge capacity in the event of a health emergency; (3) plan for just allocation of services under conditions of shortage; (4) develop a broad capability for a wide range of medical countermeasures (vaccines and pharmaceuticals); and (5) plan for the use of traditional public health strategies to reduce risk to the population. These measures may lack the glamour or political allure of planning to rescue the country from a few frightening diseases, but what they lack in glamour they gain in effectiveness because they deal with the most common and likely causes of illness and death in the population.

Build Public Health Capacity

Even with all the biosecurity funding, a miniscule proportion of health spending (1-2%) is devoted to prevention and population-based services, even though spending on upstream causes of disease are much more cost-effective. Researchers find that a small strategic investment in disease prevention could result in significant savings in U.S. health care costs. An investment of $10 per person per year in proven community-based programs could save the country more than $16 billion annually within five years, with a return of $5.60 for every $1 spent. n24

The resources spent on disease-specific threats, moreover, tend to create silos within public health agencies. These programs are not very effective for two reasons. They are directed primarily toward a single health threat, draining the agencys ability to deal with current or emergent health hazards. Thus, while they may prove beneficial against that particular hazard in the unlikely event that it does occur, they sap attention and resources from work on current needs (e.g., HIV, TB, tobacco, obesity) and future threats (e.g., emerging and resurgent infectious diseases and bioterrorism) that may save many more lives. They also tend to be time-limited, so that once the government moves onto the next health threat that garners attention in the media, whatever it might be, the funding for current programs dries up. This is a cause of great frustration to public health professionals seeking sustainable and scalable programs for disease prevention and health promotion.

Leading administration officials argue that specific programs, such as those devoted to anthrax, smallpox, and pandemic influenza, do create overall capacity. Although this is true to a certain extent, the value added to health system capacity is much lower than if the money were devoted specifically to that purpose. Moreover, when state health departments started using the idea of dual capacity to signify their intent to use bioterrorism grants for broader capacity building, the DHHS disapproved, requiring the funds to be spent strictly for the activities specified in the grant.

Building public health capacity includes the following core services: (1) public health *research* to gain knowledge of the most cost-effective measures to prevent and contain health threats; (2) *surveillance* for a broad range of pathogens and other health threats to ensure early detection; (3) *laboratories* to test pathogens and other causes of illness and death, including drug-resistant strains; (4) a well trained and financed public health *workforce*; (5) trained teams to assess, investigate, and respond to disease *outbreaks*; and (6) plans and facilities for a rapid and effective public health *response* to disease threats, including conventional strategies, such as separation of the sick from the

healthy. Devoting significant resources to build a public health infrastructure would have the dual benefits of strengthening programs for current health threats and also detecting and responding to a broad array of health emergencies should they arise. n25

Build Health Care System Capacity

Health spending in the United States rose to above $2 trillion in 2006 and has nearly doubled in the past decade, amounting to an average of $7,000 per person. This represents 16% of the total national output of good and services, nearly twice the amount spent in comparable developing countries. n26 This level of spending should produce the kind of capacity necessary to deal adequately with current needs, as well as provide a margin of safety in a public health emergency. However, the reverse is probably true because an inordinate amount of the resources is devoted to high technology solutions for relatively few individuals or spent during the last six to twelve months of life. Nearly forty-six million Americans, or 15.3% of the population, are without health insurance, n27 and a further twenty-five million are underinsured. n28 This is not simply a problem of equity, but more fundamentally one of security for the nation in the event of an epidemic or bioterror attack with a transmissible agent.

During an epidemic, whether naturally occurring or deliberate, the health care system performs at least three critical public health tasks: detection, containment, and treatment. Early detection is essential so that effective countermeasures can be initiated before the epidemic escalates. However, the early warning system will fail if patients stay away from physicians and hospitals because they are uninsured. Even if all Americans cannot obtain full health insurance, significant barriers to seeking evaluation for suspected infectious illnesses should be reduced. Any threats of deportation or financial loss due to testing for and reporting infectious illnesses should be removed, and the cost for these evaluations should be borne by the government as a necessary national security expense. n29

The task of containment is important because physicians may have to take rapid action to report a person with an infectious agent to public health authorities and initiate isolation or quarantine. Containment might fail if physicians view themselves only as advocates for individual patients, ignoring their social obligations as health professionals.

The task of administering effective treatment is the most traditional and well accepted function of the health care system. Treatment benefits not only the individual but also the community because a person under treatment for most infectious diseases is likely to be less infectious to others. However, treatment might fail if physicians do not accept their professional duty to treat patients during epidemics. During the SARS outbreaks, for example, many physicians refused to work with SARS patients, fearing for their own health and the health of their families. Thus, an ethical, and perhaps legal, obligation should be placed on health care professionals to treat exposed or infected patients during a public health emergency.

Ensure Surge Capacity in a Public Health Emergency

Even if the health system has adequate capacity to meet ongoing demands for prevention, care, and treatment, there will undoubtedly be a need for a surge of capacity during a public health emergency. Whether caused by a natural disaster, terrorism, or an infectious agent, a catastrophic event will result in mass casualties, far beyond those that hospitals can deal with unless they have an influx of resources. Everything from bandages, antibiotics, and blood for transfusions to ventilators and hospital beds will be needed to cope with a major event. Thus, government, together with its partners in the health system, should consider ways to get critical supplies to physicians and patients in the time of dire need.

This entails having stockpiles of critical equipment and supplies, together with plans to get them to areas in need rapidly. There also should be plans for ensuring that human resource needs are met by facilitating the movement of physicians, nurses, lab technicians, and other professionals to the scene of a disaster.

Fair Allocation Under Conditions of Scarcity

Government can do a great deal to help ensure surge capacity, but what is certain is that there will be extreme scarcity of countermeasures in the short term. One of the most challenging questions facing society is how to ration scarce, life-saving resources: Who shall live when not all can live? n30 Blind justice might dictate a random allocation of scarce interventions (e.g., a lottery or first-come-first served). Yet, this seems unsatisfying when lifesaving countermeasures can be targeted more cost-effectively. American society has often accepted need as the singular principle for ethical allocation--e.g., the sick or elderly. Given the devastating social, economic, and political ramifications of a serious pandemic, the following rationing criteria are worth consideration.

1. *Prevention/Public Health*. The historic mission of public health is prevention, so countermeasures to impede transmission should be a high priority. Thus, where feasible, rapid deployment of vaccines or prophylaxis to groups at risk of acquiring infection should be used to contain localized outbreaks. For example, ring vaccination of direct contacts in a family, congregate setting, or local community could be an effective intervention that would maximize lives saved.

2. *Scientific/Medical Functioning*. If the first political priority is public health, then it is essential to protect individuals who innovate and produce vaccines or antivirals, provide treatment, and protect the publics health. These are critical social missions necessary to save lives and provide care for the sick. Consequently, priority should be given to key personnel in developing countermeasures (scientists, laboratory workers), delivering health care (nurses, physicians, hospital staff), and devising public health strategies (epidemiologists, health officials).

3. *Social Functioning/Critical Infrastructure*. A pandemic could result in key sectors of society not being able to function. Many public and private actors are necessary for the publics health and safety: first responders (ambulance, fire, humanitarian assistance), security (police, national guard, military), essential products/services (water, food, pharmacies), critical infrastructure (transportation, utilities, telecommunications), and sanitation (undertakers, garbage processors, infectious waste handlers). Continued functioning of governance structures such as the executive, legislative, and judicial systems similarly would be important.

4. *Medical Need/Vulnerability*. As mentioned, medical need is a widely accepted rationing principle. This criterion focuses on reducing serious illness and death among individuals and, therefore, targets those most vulnerable. It requires a scientific or epidemiologic judgment about at-risk groups that may vary.

5. *Intergenerational Equity*. The medical need criterion often favors the elderly because they are most vulnerable to disease complications. However, there may be reasons not to routinely favor this age group. Interventions may be less beneficial to the elderly than to younger, healthier populations. Vaccines, for example, may be less effective in older people due to poor immune system function. All human lives have equal worth, but interventions targeted toward the young may save more years of life. Would a fair innings principle militate in favor of children, young adults, and pregnant women?

6. *Social Justice/Equitable Access*. The allocation of benefits should not favor the rich, powerful, or politically connected. The Gulf Coast hurricanes seared into the American consciousness the inequities that could ensue in a public health emergency--evacuation and relief services disfavored the poor and minorities. Special efforts, therefore, should be made to ensure fair distribution of lifesaving countermeasures to traditionally underserved populations.

The Model State Emergency Health Powers Act: Public Health and Civil Liberties in Conflict

In the midst of the anthrax attacks in 2001, the CDC asked the Centers for Law and the Publics Health at Georgetown and Johns Hopkins Universities to draft what became known as the Model State Emergency Health Powers Act (MSEHPA). It addresses five key public health functions discussed in this Commentary: preparedness and planning, surveillance, management of property, protection of persons, and communication and public information. The MSEHPA is designed to standardize and clearly delineate the powers states have when responding to public health emergencies. It was also drafted in recognition of the fact that most public health statutes pre-dated modern judicial

conceptions of individual rights, so it provides clearer standards and stronger guarantees of due process. n31

Under the MSEHPA, coercive public health powers can be exercised in response to an outbreak only after the governor has declared a state of emergency. A declaration gives public health officials the power to carry out examinations necessary for diagnosis and treatment. Authorities have to power to conduct isolation and quarantine when warranted to prevent a substantial risk of transmission of infection, but must adhere to human rights principles: the least restrictive alternative, safe and habitable environments, and fulfillment of individual needs for medical treatment and necessities of life. Although the MSEHPA was created with recognition that exigencies may prevent a pre-detention hearing, the government is required to petition for a court order within ten days of issuing a quarantine or isolation directive, and detainees have the right to counsel.

The MSEHPA had considerable political success, as thirty-seven states adopted it in whole or in part. Nonetheless, it provoked a storm of controversy, raising age-old concerns about public health versus civil liberties. Some scholars criticized the MSEHPA for insufficient protection of individual rights, particularly those concerning quarantine; other scholars argued that coercive powers are often ineffective and may cause health workers to under-rely on medical countermeasures; while still others expressed concern that extraordinary powers might be used in response to routine public health events. The MSEHPA, in an era of deep concern about terrorism and civil liberties, became a lightning rod for debates about public health preparedness and conformance with the rule of law. n32

In thinking about public health preparedness for the future, we should learn from the lessons of history since the attacks on the World Trade Center and anthrax outbreaks. History teaches us that it is unwise to focus on what is politically salient at the moment, lurching from one disease to the next, because that particular health hazard may never transpire. Rather, the goal should be to build a strong public health and health care infrastructure to defend against a broad range of health hazards. This will entail strong incentives for biotechnology to ensure a steady pipeline of innovative vaccines and pharmaceuticals; investing in the core functions of state and local public health departments for early detection and rapid response to all hazards; ensuring that everyone has access to high quality health care; preparing for surge capacity in the event of a mass disaster; and responding to a public health emergency on the basis of social justice, with fair allocation of scarce resources and particular attention to the needs of the least advantaged.

In exercising public health powers, it will sometimes be necessary to use compulsion, but only as a last resort. And when compulsory powers are exercised, due regard should be given for the rights and liberties of individuals. Above all, public health powers, even when society is most at risk, should be exercised under the rule of law and in accordance with the principles of social justice.

Return to Text

n1 David P. Fidler & Lawrence O. Gostin, Biosecurity in the Global Age: Biological Weapons, Public Health, and the Rule of Law (Palo Alto: Stanford Univ. Press 2008).

n2 Christopher Nelson, et al., *Conceptualizing and Defining Public Health Emergency Preparedness*, 97 (Supp. 1) Am. J. Pub. Health S9-S11 (2007).

n3 Institute of Medicine Council, Statement on Vaccine Development, in Institute of Medicine, Biological

Threats and Terrorism: Assessing the Science and Response Capabilities: Workshop Summary (2002).

n4 Pub. L. No. 108-276, *118 Stat. 835.*

n5 Gigi Kwik Gronvall, *Biodefense Countermeasures: The Impact of Title IV of the U.S. Pandemic and All-Hazards Preparedness Act*, Emerging Health Threats Journal (2008) 1:e3. doi: 10.3134/ehtj.08.003.

n6 Pub. L. No. 109-417, *120 Stat. 2831 (2006); see* James G. Hodge, Jr, Lawrence O. Gostin & Jon S. Vernick, *The Pandemic and All-Hazards Preparedness Act: Improving Public Health Emergency Response, 297 JAMA 1708-11 (2007).*

n7 The National Response Plan has been replaced by the National Response Framework, *available at* www.dhs.gov/xprepresp/committees/editorial_0566.shtm or www.fema.gov/emergency/nrf, which gives the DHS the same responsibilities.

n8 Lawrence O. Gostin, Public Health Law: Power, Duty, Restraint (2d ed. 2008).

n9 *297 F. Supp. 2d 119 (D.D.C. 2003).*

n10 Biological Products; Bacterial Vaccines and Toxoids; Implementation of Efficacy Review, *69 Fed. Reg. 255* (Jan. 5, 1999).

n11 *Doe v. Rumsfeld, 341 F. Supp. 2d 1 (D.D.C. 2004).*

n12 Y. Zhang et al., *Plasmid-Based Vaccination With Candidate Anthrax Vaccine Antigens Induces Durable Type 1 and Type 2 T-Helper Immune Responses*, 26 Vaccine 614-22 (2008).

n13 *See, e.g.*, U.S. Government Accountability Office, GAO-08-88, **Project BioShield:** Actions Needed to Avoid Repeating Past Problems with Procuring New Anthrax Vaccine and Managing the Stockpile of Licensed Vaccine (Oct. 23, 2007).

n14 David Willman, *Scientists elaborate on the case against Bruce Ivins*, L.A. Times, Aug. 19, 2008, at A9.

n15 Eric Lipton & Scott Shane, *Anthrax case renews questions on bioterror effort and safety*, N.Y. Times, Aug. 3, 2008, at A1.

n16 Advisory Committee on Immunization Practices, *Recommendations for Using Smallpox Vaccine in a Pre-Event Vaccination Program*, 52 Morbidity & Mortality Wkly. Rep. 1-16 (2003).

n17 Committee on Smallpox Vaccination Program Implementation, The Smallpox Vaccination Program: Public Health in an Age of Terrorism (2005), *available at* http://books.nap.edu/catalog.php?record_id=11240.

n18 Am. Public Health Assn, Policy Statement on Smallpox Vaccination, *available at* http://www.apha.org/legislative/policy/smallpox.htm.

n19 U.S. Dept of Health & Human Services, HHS Pandemic Influenza Plan, *available at* http://www.hhs.gov/pandemicflu/plan/; White House, National Strategy for Pandemic Influenza, *available at* http://www.whitehouse.gov/homeland/nspi.pdf.

n20 World Health Organization, No. WHO/CDS/CSR/GIP/2005.5, Global influenza preparedness plan (WHO: Geneva 2005), *available at* www.who.int/csr/resources/publications/influenza/GIP_2005_5Eweb.pdf.

n21 Patricia M. Danzon et al., *Vaccine Supply: A Cross-National Perspective*, 24 Health Affairs 706-17 (2005).

n22 Lawrence O. Gostin & Benjamin E. Berkman, *Pandemic Influenza: Ethics, Law, and the Publics Health, 59 Admin. L. Rev. 121-75 (2007), available at* http://lsr.nellco.org/georgetown/fwps/papers/19.

n23 Lawrence O. Gostin, *When Terrorism Threatens Health: How Far are Limitations on Personal and Economic Liberties Justified? 52 Fla. L. Rev. 1-65 (2003).*

n24 Trust for Americas Health, Prevention for a Healthier America: Investments in Disease Prevention Yield Significant Savings, Stronger Communities (2008).

n25 Institute of Medicine, The Future of the Publics Health in the 21st Century (2003).

n26 Aaron Catlin et al., *National Health Spending In 2006: A Year Of Change For Prescription Drugs*, 27 Health Affairs 14-29 (2008).

n27 Carmen DeNavas-Walt, Bernadette D. Proctor & Jessica C. Smith, Income, Poverty, and Health Insurance Coverage in the United States: 2007: U.S. Census Bureau, Current Population Reports, P60-235 (2008), *available at* http://www.census.gov/prod/2008pubs/p60-235.pdf.

n28 Cathy Schoen, Sara R. Collins, Jennifer L. Kriss, & Michelle M. Doty, How Many Are Underinsured? Trends Among U.S. Adults, 2003 and 2007, Health Affairs Web Exclusive, June 10, 2008, *available at* http://www.commonwealthfund.org/publications/publications_show.htm?doc_id=688615.

n29 Matthew K. Wynia & Lawrence Gostin, *The Bioterrorist Threat and Access to Health Care*, 296 Science 1613 (May 31, 2002); Matthew K. Wynia & Lawrence O. Gostin, *Ethical Challenges in Preparing for Bioterrorism: Barriers Within the Health Care System*, 94 Am. J. Pub. Health 1096-1102 (2004).

n30 John D. Arras, *Rationing Vaccine During An Avian Influenza Pandemic: Why It Wont Be Easy*, 78 Yale J. Biol. & Med. 287300 (2005).

n31 Lawrence O. Gostin, *Public Health Law in an Age of Terrorism: Rethinking Individual Rights and Common Goods*, 21 Health Affairs 79-93 (2002).

n32 *Compare* Lawrence O. Gostin, *The Model State Emergency Health Powers Act: Public Health and Civil Liberties in a Time of Terrorism*, *13 Health Matrix 3-32 (2003), with* Wendy E. Parmet, *Quarantine Redux: Bioterrorism, AIDS, and the Curtailment of Individual Liberty in the Name of Public Health*, *13 Health Matrix 85-116 (2003).*

RELATED LINKS: For more information see
- 42 U.S.C. §§ 247d-3a;
- 264.

On Smallpox Emergency Personnel Protection, see
- 42 U.S.C. §§ 239-239h.

On the Smallpox Compensation Program, see
- 42 C.F.R. §§ 102.1-102.92.

And for the National All-Hazards Preparedness Public Health Emergencies statutes, see
- 42 U.S.C. §§ 300hh to 300hh-16.

ABOUT THE AUTHOR(S):

Lawrence O. Gostin is the Linda D. and Timothy J. ONeill Professor of Global Health Law at the Georgetown University Law Center, where he directs the ONeill Institute for National and Global Health Law. Dean Gostin is also Professor of Public Health at the Johns Hopkins University and Director of the Center for Law & the Publics Health at Johns Hopkins and Georgetown Universities--a Collaborating Center of the World Health Organization and the Centers for Disease Control and Prevention. Dean Gostin is Visiting Professor of Public Health (Faculty of Medical Sciences) and Research Fellow (Centre for Socio-Legal Studies) at Oxford University. He is the Health Law and Ethics Editor, a contributing writer, and a columnist for the *Journal of the American Medical Association*. In 2007, the Director General of the World Health Organization appointed Dean Gostin to the International Health Regulations (IHR) Roster of Experts and the Expert Advisory Panel on Mental Health.

Dean Gostin has a B.A. from the State University of New York-Brockport and a J.D. from Duke University. He also has three honorary degrees. In 1994, the Chancellor of the State University of New York conferred an Honorary Doctor of Laws Degree. In 2006, he was awarded Cardiff Universitys (Wales) highest honor, being made an Honorary Fellow. In 2007, the Royal Institute of Public Health designated Dean Gostin as a Fellow of the Royal Society of Public Health (FRSPH).

Dean Gostin, an elected lifetime Member of the Institute of Medicine/National Academy of Sciences, serves on the Board on Health Sciences Policy and the Committee on Science, Technology, and Law. He currently chairs the Institutes Committee on Health Informational Privacy, and has chaired committees on genomics and on prisoner research. The Institute awarded Dean Gostin the Adam Yarmolinsky Medal for distinguished service to further its mission of science and health. He received the Public Health Law Associations Distinguished Lifetime Achievement Award in recognition of a career devoted to using law to improve the publics health presented at the CDC. Internationally, Dean Gostin received the Rosemary Delbridge Memorial Award from the National Consumer Council (U.K.) for the person who has most influenced Parliament and government to act for the welfare of society. He also

received the Key to Tohoko University (Japan) for distinguished contributions to human rights in mental health.

Dean Gostin has led major law reform initiatives in the United States, including the drafting of the Model Emergency Health Powers Act to combat bioterrorism and the Turning Point Model State Public Health Act. He is also leading a drafting team on developing a Model Public Health Law for the World Health Organization.

In the United Kingdom, he was the Legal Director of the National Association for Mental Health, Director of the National Council of Civil Liberties (the UK equivalent of the ACLU), and a Fellow at Oxford University. He helped draft the current Mental Health Act (England and Wales) and brought several landmark cases before the European Commission and Court of Human Rights.

Dean Gostins latest books are: *Public Health Law: Power, Duty, Restraint* (University of California Press and Milbank Memorial Fund, 2d ed. 2008); *Public Health Ethics: Theory, Policy and Practice* (Oxford University Press, 2007); *The AIDS Pandemic: Complacency, Injustice, and Unfulfilled Expectations* (University of North Carolina Press, 2004); *The Human Rights of Persons with Intellectual Disabilities: Different But Equal* (Oxford University Press, 2003); *Public Health Law and Ethics: A Reader* (University of California Press and Milbank Memorial Fund, 2002).

More information is at http://www.law.georgetown.edu/faculty/gostin/index.html (Dean Gostin) and http://www.publichealthlaw.net/index.php (the Centers for Law & the Publics Health).

Jennifer M. Chacon on Border Searches of Electronic Data

2008 Emerging Issues 2430

Jennifer M. Chacon on Border Searches of Electronic Data

By Jennifer M. Chacon

June 30, 2008

SUMMARY: Recent court cases and news articles have dwelt on people arriving in the United States who had a laptop, disk, or other computer gear seized and searched by customs officials. Jennifer M. Chacn, who teaches criminal and immigration law at the University of California-Davis law school, explains why the government can do this, the constitutional standard that applies, and what the ramifications are and can yet be.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Cite as: Chacon, Jennifer M. Border Searches of Electronic Data. LexisNexis Expert Commentary, *(Insert date you accessed the document online)*.

The international traveler has long faced numerous challenges, including passport and visa requirements, rising airfares, and jetlag. Now, individuals traveling with laptop computers or other electronically stored information face an additional complicating factor: They face the possibility that their laptops and electronic files may be searched or even seized by U.S. government officials when they attempt to enter the United States. For some travelers, the most surprising aspect of these border searches may be the fact that several courts to consider the question have concluded that no individualized suspicion is required for border laptop searches or seizures; that is, government officials at ports of entry can search or seize laptops and electronic data for any reason or no reason at all.

This article discusses the state of the law regarding border laptop searches. It provides an overview of the relevant constitutional case law, describes several recent court decisions explicitly analyzing the issue, and concludes with a discussion of the broader implications of these cases.

I. Border Searches: the Constitutional Framework. The Fourth Amendment of the United States Constitution provides that [t]he right of the people to be secure in their persons, houses, papers, and effects shall not be violated. n1 The Courts have interpreted the Amendment as providing people with protection from unreasonable searches and seizures by government actors. When government officials conduct a search of an area in which individuals have high expectations of privacy, such as their own homes, courts have generally interpreted the Fourth Amendment to require that such searches take place only after the issuance of a judicial warrant. n2 When conducting searches of containers and vehicles in public places, courts have not always required a warrant, but have maintained that the officers must have probable cause to believe that evidence of a crime will be found prior to conducting the search. n3 Government

officials can conduct brief detentions and pat-down searches of an individual where they have reasonable suspicion that the individual poses a danger to the safety of the officer. n4 The reasonable suspicion standard is lower than the probable cause standard, and is all that is required for a brief stop or non-intrusive, frisk-style search. n5

However, in certain contexts, courts have approved deviations from these standards. When a search is particularly intrusive, such as a search involving a blood test, the Supreme Court has suggested that government officials need more than the usual level of probable cause. n6 More often, courts have relaxed the probable cause and reasonable suspicion standards within particular contexts. For example, in public schools, school officials have been allowed to conduct searches of students belongings in the absence of probable cause. n7 Similarly, courts have upheld random drug testing of customs agents where there was no individualized suspicion about criminality because of the unique nature of the job. n8

One context in which the courts routinely have given government officials greater leeway to conduct searches is at the nations borders. n9 Courts have reasoned that searching the baggage of arriving passengers is based on [the country's] inherent sovereign authority to protect its territorial integrity. n10 Thus, although arriving passengers still have an expectation of privacy in their belongings, the governments strong interest in protecting its borders generally outweighs the individuals expectation of privacy at the border. n11 The same rationale that applies at traditional ports of entry also applies to international travelers at airport checkpoints, because such checkpoints are the functional equivalent of the border. n12 The strong governmental interest in protecting the nations territorial interest trumps an individual's privacy interests in most border searches. The Supreme Court thus has upheld routine, suspicionless searches of the luggage of arriving passengers no matter how great the travelers desire to conceal the contents may be. n13

Nevertheless, the Court has acknowledged that there are some constitutional limits on border searches. In spite of the broad power of the government to conduct searches at the border, highly intrusive searches and searches that are conducted in a particularly offensive manner are subject to constitutional limitations. In *United States v. Montoya de Hernandez*, n14 the Court found that the search of a travelers alimentary canal, achieved by detaining the traveler for sixteen hours until she passed the drugs that she had ingested, could not be conducted in the absence of individualized suspicion. n15 Instead, the Court found that the dignity and privacy interests at stake required that such searches be conducted only where government officials had reasonable suspicion of criminal activity. n16 The Court suggested that individualized suspicion was needed to conduct any non-routine border search, such as strip, body cavity, or involuntary x-ray searches, n17 but did not specify the appropriate level of suspicion for these non-routine border searches.

Similarly, the Court has suggested that border searches that are carried out in a particularly offensive manner are not routine, and will require some degree of individualized suspicion. n18 This might include highly intrusive searches, or searches that are particularly destructive of personal property. n19 The Court has set a high bar in this regard. For example, the Court found that a search that took about an hour and required the disassembly and reassembly of the gas tank of a car was routine and therefore did not require any degree of individualized suspicion. n20

This is the legal context in which border laptop searches have unfolded. Some government officials at border checkpoints or international airport checkpoints have begun to search the laptops and other electronic information of incoming international travelers without any individualized suspicion of wrongdoing. n21 Presumably, these officials are treating these searches as part of a routine border search. This raises an interesting legal question: Are these border searches of laptops and other electronic information routine border searches, or are they sufficiently intrusive or offensive so as to require at least some degree of individualized suspicion? To date, the two circuit courts that have considered the question have concluded that such searches fall within the category of routine border searches, and can be conducted in the absence of individualized suspicion. n22

II. Laptop Searches: Routine Border Searches? Computer laptops and other electronic storage devices are different from a car or a suitcase. Such items may contain substantial amounts of personal information about the person carrying the laptop or electronic data. They may also contain other materials that raise heightened privacy concerns: A

reporter may be carrying electronic notes from confidential sources; a lawyer may have privileged legal communications; a doctor may have confidential electronic medical files; an employee may have in her electronic files trade secrets or other proprietary company information. n23 Therefore, it is not immediately obvious that the same doctrine that governs the search of a suitcase or an automobile should also govern the search of a laptop. Nevertheless, that is the position that the government has successfully argued in the two circuits that have considered the question.

On April 21, 2008, the Ninth Circuit handed down its decision in the case of *United States v. Arnold*. n24 The defendant-appellee in that case, Matthew Arnold, had arrived at Los Angeles International Airport on a flight from the Philippines. n25 He was selected for secondary questioning by U.S. Customs and Border Protection (CBP) Officer Laura Peng, who asked Arnold a series of standard questions regarding his trip, and he answered that he had been on vacation for three weeks, visiting friends. n26 Peng searched his luggage and found Arnolds laptop computer, a separate hard drive, a computer memory stick and six compact disks. n27 Peng and her colleague CBP Officer John Roberts reviewed several photo files on Arnolds computer, and when they discovered a photo that depicted two nude women, they notified a supervisor. n28 Ultimately, special agents from Immigration and Customs Enforcement (ICE) detained Arnold for several hours and questioned Arnold about the contents of his laptop. n29 When the agents discovered images that they believed to be child pornography, they seized the computer and storage device, but released Arnold. n30 Arnold was later charged with various criminal offenses relating to the possession and transportation of child pornography. n31

Arnold challenged the initial search of his laptop, arguing that the search exceeded the scope of a routine border search, that the government violated his Fourth Amendment rights by conducting this search in the absence of reasonable suspicion. n32 The district court agreed to suppress the evidence obtained in the laptop search, holding that the search of the laptop required reasonable suspicion, and the government did not have the reasonable suspicion required to search Arnolds laptop. n33 This holding was overturned by the Ninth Circuit, which concluded that the laptop search was a routine border search that did not require reasonable suspicion. n34

In reaching its conclusion, the Court observed that it was declining to create a split with the Fourth Circuits decision in *United States v. Ickes*. n35 In that case, the defendant had been stopped by ICE agents at a land border crossing along the Canadian border. In searching Ickes van, the agents reviewed a videotape in a video camera. Upon determining that Ickes videotaped tennis match focused excessively on a young ball boy, n36 the agents conducted a full search of the van, which turned up more child pornography. n37

Ickes had argued that although the Fourth Amendment allowed for routine border searches, the First Amendments protection of free speech required that a higher level of suspicion be required in cases involving the search of expressive materials. n38 The Fourth Circuit declined to create such an exception, concluding that such a rule would protect terrorist communications; would create an unworkable standard for government officials; and would run counter to a line of case law declining to apply heightened protection under the Fourth Amendment when First Amendment interests were alleged. n39

Read in combination, the *Ickes* and *Arnold* cases suggest that the governments decision to search the information on a laptop or any other electronic storage device at the border or its functional equivalent is permissible with respect to any traveler, for any legal reason or no reason at all. The *Ickes* court concluded that searches of electronic data (in that case, videotapes) require no individualized suspicion, regardless of the potentially expressive nature of the materials. The *Arnold* court embraced that reasoning, and expanded upon it. It concluded that government officials at international checkpoints can require an individual to turn on his or her laptop and can review any and all of the files therein without any individualized suspicion.

The *Arnold* court not only rejected the use of a more protective standard under a First Amendment rationale, but also developed an explanation as to why this kind of search constituted a routine border search. In the view of the Ninth Circuit, the case law established two kinds of searches that were potentially not routine. The first is an intrusive search of the body. n40 The second is a highly offensive search, which the court defined to encompass only those searches

that involved destruction of property. n41 Since a search of a laptop involves neither, n42 that search was analogous to luggage searches, car searches, and other routine border searches that require no individualized suspicion.

The rationale of the Ninth Circuit is supported by the case law, but it is not indisputable. First, the court reasoned that the *Flores-Montano* case stood for the proposition that only searches of the body could constitute a highly intrusive search of the person. n43 Second, the Ninth Circuit concluded, again citing *Flores-Montano*, that a search of property can never be highly intrusive unless it results in damage to the property. n44 Although the *Flores-Montano* case can be read to support both of these propositions, it by no means requires the conclusion reached by the Ninth Circuit with respect to the first proposition.

The Court in *Flores-Montano* did reject the suggestion that a search of a gas tank was sufficiently intrusive to constitute a violation of the defendants privacy interest, but used language that arguably does not apply to the contents of a laptop computer. The court wrote that [i]t is difficult to imagine how the search of a gas tank, which should be solely a repository for fuel, could be more of an invasion of privacy than the search of the automobiles passenger compartment. n45 In contrast, it is not at all difficult to imagine that the search of the files contained on a laptop could be more an invasion of privacy than the search of a passenger compartment, or even a suitcase. Computers increasingly contain vast amounts of personal information. n46 A more appropriate (although still imperfect) analogy might be made to first class mail, and courts have required customs officials to have reasonable suspicion before opening international first class mail. n47

Moreover, contrary to the Ninth Circuits suggestion in *Arnold*, the *Flores-Montano* case did not definitively rule out the possibility of applying a balancing test to determine whether or not a border search was routine or more intrusive. *Flores-Montano* held that such balancing tests, while required for searches of persons, were not required for searches of vehicles. n48 One might argue that a search of the very personal contents of a laptop computer warrant the application of a balancing test, even if such balancing is inappropriate for a vehicle search. A search need not involve an invasion of the physical body to be intrusive. n49 Nevertheless, only District Judge Pregerson, who decided the case that was ultimately overruled by the Ninth Circuit, has decided to date that laptop searches are non-routine and require individualized suspicion. n50

III. Implications of the Border Search Cases. For the international traveler, the decision by several courts to uphold searches by government agents of laptop and other electronic files at the border with no individualized suspicion whatsoever has serious implications. The *Arnold* case and the *Ickes* case each reaffirm a practice that is already widespread: one in which customs and immigration officials routinely search, download, and save electronic files at the border and its functional equivalent. As the Association of Corporate Travel Executives and the Electronic Frontier Foundation noted in their amici brief to the Ninth Circuit in the *Arnold* case, that case and other recent cases have involved instances where [c]ustoms officials in fact conduct sophisticated searches of seized computers, looking at documents, deleted files, and Internet caches. n51 International travelers need to be aware that customs and immigration agents currently are exercising their apparent authority to search, copy, and store the contents of travelers laptops even if there is no reason for the government to suspect that the individual carrying that laptop is in any way involved in criminal activity.

This broadly permissive policy carries potential risks. First, it means that travelers whose laptops or other electronic files contain confidential or otherwise sensitive information cannot carry these items across borders with any assurance that the contents will not be reviewed and stored by government officials upon re-entry or entry into the United States. n52 Second, it means that business travelers who rely on company computers may be held accountable at border checkpoints for content on those laptops, even if they had nothing to do with creating that content. n53

Finally, in the absence of any requirement for individualized suspicion, there is a chance that electronic files will be searched arbitrarily, unnecessarily, or even in ways that reflect patterns of racial profiling. This concern was raised in a recent civil lawsuit filed by the Electronic Frontier Foundation and the Asian Law Caucus. n54 The complaint alleged that the Department of Homeland Security has failed to comply with requests for public records sought under the

Freedom of Information Act, and the relief sought includes government disclosure of its border search policies, including which rules govern the seizing and copying of the contents of electronic devices. n55

In short, international travelers should be aware that the contents of their electronic files, no matter how personal or insignificant, currently are subject to random and routine search at international borders. Unless the courts or Congress reevaluate the policy, the traveler who wants to protect private electronic information in any form would be best served by refraining from carrying that information across the international border.

Additional information

United States v. McAuley, DR-07-CR-786(1)-*AML, 2008 U.S. Dist. LEXIS 44688* (June 6, 2008) (court holds search of personal computer and "disks, hard drives, or other technical devices" at port of entry a routine search, not requiring reasonable suspicion).

Laptop Searches and Other Violations of Privacy Faced by Americans Returning from Overseas Travel: Hearing of Before the Subcomm. on the Constitution, Civil Rights and Property Rights, S. Comm. on the Judiciary, 110th Cong. (June 25, 2008), *at* http://judiciary.senate.gov/hearing.cfm?id=3420.

Yule Kim, Congressional Research Service, RL 34404, Border Searches of Laptops and Other Electronic Storage Devices (Mar. 5, 2008).

John Wesley Hall, 2 Search and Seizure ch. 26.

Judith Blakley, *Can U.S. Customs Search & Seize Your Laptop Computer Without Cause? YES They Can!*, Associatedcontent.com, Nov. 11, 2006, http:// www.associatedcontent.com/ article/82561/canuscustomssearchseizeyour laptop.html.

Jennifer Granick, *Computer Privacy in Distress*, WIRED, Jan. 17, 2007, http://www.wired.com/ politics/law/commentary/circuitcourt/2007/01/72510.

Press Release, Association of Corporate Travel Executives, ACTE and EFF Seek Reversal of Laptop Seizure Decision in Second Amicus Brief (June 12, 2008), *available at* http://www.acte.org/resources/press_release.php?id=311.

Press Release, Electronic Frontier Foundation, Civil Liberties Groups Sue Homeland Security for Records on Intrusive Questioning and Searches of U.S. Travelers: Information Sought in Response to Growing Complaints of Harassment at U.S. Borders (Feb. 7, 2008), *available at* http://www.eff.org/press/archives/2008/02/07.

Return to Text

n1 . U.S. Const. amend. IV.

n2

[2]. *See Kyllo v. United States, 533 U.S. 27 (2001); cf. Payton v. New York, 445 U.S. 573, 590 (1980)* (The Fourth Amendment draws a firm line at the entrance to the house.). The Supreme Court has approved warrantless entries into the home in cases involving exigent circumstances. *See, e.g., Warden v. Hayden, 387 U.S. 294 (1967).*

n3

[3]. *See, e.g., California v. Acevedo, 500 U.S. 565 (1991)* (allowing warrantless search of a container in a vehicle upon probable cause); *California v. Carney, 471 U.S. 386 (1985)* (allowing warrantless search of a mobile home on probable cause); *Chambers v. Maroney, 399 U.S. 42 (1970)* (requiring probable cause for a warrantless search of a car); *Carroll v. United States, 267 U.S. 132 (1925)* (same).

n4

[4]. *Terry v. Ohio, 392 U.S. 1 (1968).*

n5

[5]. *Id. at 27-31*.

n6

[6]. *See, e.g., Schmerber v. California, 384 U.S. 757, 769 (1966)* (requiring a clear indication that incriminating evidence will be found before a blood sample is drawn for evidence).

n7

[7]. *New Jersey v. T.L.O, 469 U.S. 325, 341-42 (1985)* (allowing full search of students personal belongings where there is reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school).

n8

[8]. *National Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989).*

n9

[9]. *United States v. Flores-Montano, 541 U.S. 149, 153 (2004); United States v. Ramsey, 431 U.S. 606, 616 (1977).*

n10

[10]. *Torres v. Puerto Rico, 442 U.S. 465, 472-73 (1979).*

n11

[11]. *See, e.g., Flores-Montano, 541 U.S. at 153* (It is axiomatic that the United States, as sovereign, has inherent authority to protect, and a paramount interest in protecting, its territorial integrity.).

n12

[12]. *Almeida-Sanchez v. United States, 413 U.S. 266, 273 (1973).* Some circuit courts also have adopted an extended border search doctrine, under which border searches that occur near the border are deemed constitutionally permissible if reasonable under the *Fourth Amendment. United States v. Yang, 286 F.3d 940, 945 (7th Cir. 2002); see also United States v. Ogbuehi, 18 F.3d 807, 813 (9th Cir. 1994)* (treating secondary inspection as a routine border search although it occurred a few minutes after defendant had crossed the border, and sixty feet away); *United States v. Wardlaw, 576 F.2d 932, 935 (1st Cir. 1978)* (finding that a secondary inspection at the border site, after a border inspection, was still a routine border search).

n13

[13]. *United States v. Ross, 456 U.S. 798 (1982).*

n14

[14]. *473 U.S. 531 (1985).*

n15

[15]. *Id. at 541.*

n16

[16]. *Id.*

n17

[17]. *Id. at 541, n.4.*

n18

[18]. *Flores-Montano, 541 U.S. at 155, n.2.*

n19

[19]. *Id. at 155-56.*

n20

[20]. *Id.*

n21

[21]. Joe Sharkey, *At U.S. Border, Laptops Have No Right to Privacy*, N.Y. Times, Oct. 24, 2006, at C8; *see also* Adam Liptak, *Sidebar: If Your Hard Drive Could Testify*, N.Y. Times, Jan. 7, 2008, at A12 ([T]he government contends that it is perfectly free to inspect every laptop that enters the country, whether or not there is anything suspicious about the computer or its owner.). In addition, at least one passenger was *leaving* the United States when her laptop was seized for investigation and not returned. Ellen Nakashima, *Clarity Sought on Electronic Searches; Travelers Devices Seized at Border*, Wash. Post, Feb. 7, 2008, at A1.

n22

[22]. *United States v. Arnold, 523 F.3d 941 (9th Cir. 2008)* (holding that a search of files on a laptop constituted a routine border search); *United States v. Ickes, 393 F.3d 501, 506-08 (4th Cir. 2005)* (holding that the inspection of videotape in defendants van constituted a routine border search).

n23

[23]. *United States v. Arnold, 454 F. Supp. 2d. 999, 1003-04 (C.D. Cal. 2006).*

n24

[24]. *United States v. Arnold, 523 F.3d 941 (9th Cir. 2008).* The Ninth Circuit had previously answered in the affirmative the question of whether a laptop search constituted a routine border search. *United States v. Romm, 455 F.3d 999 (9th Cir. 2006).* However, in that case, Romm failed to raise the argument that the search was too intrusive to constitute a routine search until his reply brief on appeal, and the Ninth Circuit declined to consider the issue. *Id.* at 997.

n25

[25]. *Id.* at 943.

n26

[26]. *Id.*

n27

[27]. *Id.*

n28

[28]. *Id.*

n29

[29]. *Id.*

n30

[30]. *Id.*

n31

[31]. *Id.*

n32

[32]. *Id.*

n33

[33]. *United States v. Arnold, 454 F. Supp. 2d. 999 (C.D. Cal. 2006).*

n34

[34]. *Arnold, 523 F.3d at 946* ([W]e are satisfied that reasonable suspicion is not needed for customs officials to search a laptop or other personal electronic storage device at the border.).

n35

[35]. *393 F.3d 501 (4th Cir. 2005).*

n36

[36]. *Id. at 502.*

n37

[37]. *Id. at 503.*

n38

[38]. *Id. at 506.*

n39

[39]. *Id. at 506-08.*

n40

[40]. *Arnold, 523 F.3d at 945.*

n41

[41]. *Id.*

n42

[42]. *Id.*

n43

[43]. *Id. at 945-46.*

n44

[44]. *Id. at 945.*

n45

[45]. *Flores-Montano, 541 U.S. at 154.*

n46

[46]. Orin Kerr, *Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 569 (2005)* (As computers become involved in more aspects of our lives, they record increasingly diverse information. Each

new software application means another aspect of our lives monitored and recorded by our computers.)

n47

[47]. *United States v. Ramsey, 431 U.S. 606, 616-19 (1977).*

n48

[48]. *Flores-Montano, 541 U.S. at 152.*

n49

[49]. *See, e.g., United States v. Mejia, 720 F.2d 1378, 1382 (5th Cir. 1983)* (intrusion is keyed to embarrassment, indignity, and invasion of privacy). In *Mejia*, the Fifth Circuit upheld the use of X-rays upon reasonable suspicion that the defendant had ingested drugs. Interestingly, the court distinguished the use of X-rays from a physical invasion of the body, but still required reasonable suspicion for that search. *Id. at 1382.*

n50

[50]. *United States v. Arnold, 454 F. Supp. 2d. 999 (C.D. Cal. 2006) overruled by United States v. Arnold, 523 F.3d 941 (9th Cir. 2008).* Several other district courts have reached the opposite conclusion. *See, e.g., United States v. Irving, 2003 U.S. Dist. LEXIS 16111* (S.D.N.Y. Sept. 15, 2003), *affd on other grounds, 452 F.3d 110, 124 (2d Cir. 2006); United States v. Roberts, 86 F. Supp. 2d 678 (S.D. Tex. 2000), affd on other grounds, 274 F.3d 1007 (5th Cir. 2001).* At least one of these courts has analogized computers to closed containers, which are frequently subjected to routine border searches. *Irving, 2003 U.S. Dist. LEXIS 16111,* at *14-*15. The circuit courts that reviewed these cases determined that ICE officials had reasonable suspicion to conduct the search, thus eliminating the need to characterize these searches as routine border searches. *See, e.g., United States v. Irving, 452 F.3d 110, 124 (2d Cir. 2006)* (finding that the border search of computer diskettes and film took place after agents had developed reasonable suspicion); *United States v. Roberts, 274 F.3d 1007, 1012 (5th Cir. 2001)* (declining to adopt expressly the district courts conclusion that the extensive search of, *inter alia,* Robertss computer and diskettes constituted a routine border search, but deciding that the agents had reasonable suspicion to conduct the search). At least one district court has taken a similar approach. *United States v. Furukawa, 2006 U.S. Dist. LEXIS 83767* (D. Minn. Nov. 16, 2006). At least one other district court has simply assumed without discussion that such searches are routine border searches. Bagley v. United States, No. C05-1161-JCC-JPD (W.D. Wash. Jan. 23, 2006) (Customs agents conducted a routine border search and discovered images of child pornography on Petitioners laptop.).

n51

[51]. Brief for Amici Curiae Association of Corporate Travel Executives and Electronic Frontier Foundation in Support of Defendant-Appellee at 19, United States v. Arnold, No. 06-50581 (9th Cir. June 19, 2007) (*available at* http://www.eff.org/cases/us-v-arnold).

n52

[52]. In their amici brief in the Arnold case, the Corporate Travel Executives and Electronic Frontier Foundation also noted that they d[id] not know whether or how the copied contents of seized computers are reviewed, stored, and shared with other government agencies." *Id.* at 8 & n.2.

n53

[53]. *Id.* at 16-17 & n.4; *cf.* Ellen Nakashima, *Clarity Sought on Electronic Searches; Travelers Devices Seized at Border*, Wash. Post, Feb. 7, 2008, at A1 (one man, asked to provide his password, pointed out that it was not his computer, but his company's).

n54

[54]. Ellen Nakashima, *Clarity Sought on Electronic Searches; Travelers Devices Seized at Border*, Wash. Post, Feb. 7, 2008, at A1.

n55

[55]. *Id.* The complaint is available at http://www.eff.org/cases/foia-litigation-border-searches. Asian Law Caucus v. United States Department of Homeland Security, No. CV 08 0842 (N.D. Cal. filed Feb. 7, 2008).

ABOUT THE AUTHOR(S):

Jennifer M. Chacon is a Professor of Law at the University of California, Davis, King Hall School of Law, where she teaches Immigration Law, Criminal Procedure, and Criminal Law. Prior to her appointment at King Hall, Professor Chacon was an associate at the law firm of Davis, Polk & Wardwell (1999-2003) and a law clerk to the Honorable Sydney R. Thomas on the Ninth Circuit's Court of Appeals (1998-1999). She received her J.D. in 1998 from Yale Law School and her A.B., with distinction, from Stanford University in 1994.

14 of 19 DOCUMENTS

Joe Whitley and Ed Britan on Chemical Facility Anti-Terrorism Standards Rule

2008 Emerging Issues 2273

Joe Whitley and Ed Britan on a New Standard for Security Regulation: The Interim Final Rule on Chemical Facility Anti-Terrorism

By Joe Whitley and Ed Britan

May 15, 2008

SUMMARY: These regulations require that facilities with threshold amounts of any of more than a hundred chemicals complete an online questionnaire to determine their risk. High-risk facilities then must do security vulnerability assessments and prepare and implement security plans. Such risk-based performance standards may become a template for future security regulation of other industries and critical infrastructures.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: *Although the Interim Final Rule on Chemical Facility Anti-Terrorism Standards was created for the security of high-risk chemical facilities, its regulatory scheme of risk-based performance standards may become a template for future security regulation in other industries and critical infrastructures.*

I. Background and Premise

On April 9, 2007, under authority delegated to it pursuant to section 550 of the Department of Homeland Security Appropriations Act of 2007, n1 the Department of Homeland Security (DHS) published its Interim Final Rule on Chemical Facility Anti-Terrorism Standards (CFATS). n2 CFATS establishes a comprehensive regulatory scheme to secure high-risk chemical facilities based upon risk-based performance standards. CFATS requires that covered facilities conduct security vulnerability assessments and prepare and implement security plans according to their particular vulnerability to terrorist attack. To assist DHS in determining whether a facility is high risk, CFATS includes an appendix, entitled DHS Chemicals of Interest (Appendix A), that specifically lists chemicals of interest and screening threshold quantities that DHS considers potentially dangerous. n3 Other than Appendix A, CFATS took effect on June 8, 2007. Appendix A became effective on November 20, 2007.

This article will summarize the various provisions of CFATS, and draw a conclusion as to the influence CFATS may have on future homeland security regulation.

II. Executive Summary

A. Risk and Consequence Assessment. DHS was granted the discretion to define what facilities are "high risk" and, therefore, what facilities will be subject to CFATS requirements. DHS will consider a facility high risk if it presents a high risk of significant adverse consequences for human life or health, national security and/or critical economic assets if subjected to terrorist attack, compromise, infiltration, or exploitation. n4 Since DHS currently lacks sufficient information to determine which facilities pose a high level of security risk, it is requiring facilities that possess (or later come into possession of) chemicals listed in Appendix A in quantities that meet or exceed the screening threshold for any applicable security issue to complete an online questionnaire known as the Top-Screen. The completed Top-Screen will allow DHS to assess the nature of the risk a facility poses and what facilities warrant high risk designation. Chemical facilities that possesses or plan to possess any of the chemicals of interest listed in Appendix A, at or above the screening threshold quantity, must register within sixty days under the Top-Screen. n5 Although DHS may independently determine that a facility is high risk, n6 in most cases, DHS will make this determination upon review of Top-Screen submissions.

A facility that DHS determines to be high risk will be referred to as a Covered Facility. n7 Depending upon the perceived risk, Covered Facilities will be placed in one of four risk tiers with commensurate performance-based security obligations. DHS will notify a facility if it has been designated to a high risk tier, and will provide general tier criteria to the facility through forthcoming guidance documents. The guidance is intended to provide acceptable layering of measures to the Covered Facility so it can meet its performance-based obligations. n8 For facilities in the top risk tiers, the recommended security measures will be more robust to provide for greater protection. The actual determination allocating a Covered Facility to a tier will be protected as chemical-terrorism vulnerability information (CVI) under CFATS. n9

B. Propane as a Chemical of Interest. In Appendix A, DHS set a special screening threshold for the chemical of interest (COI) propane because of the significant consequences it could produce if used in a terrorist attack. n10 The screening threshold for COI propane is 60,000 pounds, and facilities need not count propane in tanks of less than 10,000 pounds. In setting such a high threshold, DHS has elected to focus its security screening efforts on large commercial propane establishments, and on industrial, non-distribution facilities that use propane in their operations, rather than on non-industrial propane customers. n11

Shortly before the deadline for propane handlers meeting the screening threshold quantity to complete a Top--Screen survey, the National Propane Gas Association (NPGA) sued DHS in the United States District Court for the District of Columbia to challenge the CFATS final rules regulating propane. However, on January 20, 2008, the judge presiding in that case issued a decision denying NPGAs request for both a temporary restraining order and a preliminary injunction. In coming to its decision, the court found that the inherent harm to an agency in preventing it from enforcing regulations that Congress found it in the public interest to direct an agency to develop and enforce outweighed any and all justifications for the injunctive relief sought. n12

Upon publication of the Appendix A Final Rule, DHS received numerous inquiries about its regulation of COI propane. In response, on March 21, 2008, DHS published a Clarification to Chemical Facility Anti-Terrorism Standards; Propane, in which DHS explained that it intended COI propane to refer only to products containing at least 87.5% propane. n13

C. Obligations of Covered Facilities. A Covered Facility will be required to periodically conduct a Security Vulnerability Assessment (SVA) and then develop and execute a Site Security Plan (SSP) that must be reviewed and approved by DHS. n14 In short, the SVA identifies facility security vulnerabilities, and the SSP must address the vulnerabilities identified in the SVA and describe how the selected security measures (both physical and procedural) that are already in place, as well as those that the facility plans to implement, will address the eighteen substantive regulatory risk-based performance standards. n15 In certain circumstances, a Covered Facility is permitted to submit an Alternate Security Program (ASP), rather than an SVA or SSP or both. n16

D. SAFETY Act Implications. The Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY

Act) n17 is intended to foster the development of anti-terrorism technologies by eliminating or reducing the liability of companies whose anti-terror products or services fail to prevent or mitigate a terrorist act. Any facility that conducts vulnerability assessments or that systematically upgrades its physical security measures is eligible to receive litigation protection under the SAFETY Act. Consequently, a facility can bolster its chances of receiving the litigation protections provided by the SAFETY Act by fulfilling its obligations under CFATS.

E. Enforcement. CFATS contains provisions concerning inspections, appeals, audits, recordkeeping, and the protection of sensitive chemical-terrorism vulnerability information (CVI). n18 It also provides DHS with the authority to assess fines and, in extreme cases, to issue an order for the cessation of operations. n19 Third-party actions are not allowed under CFATS; only the Secretary of Homeland Security may pursue its remedies. n20

F. Protection of Chemical-Terrorism Vulnerability Information (CVI). Protecting sensitive information shared or developed under CFATS from public disclosure is crucial to securing chemical facilities. Such information may contain, among other things, current vulnerabilities or other details of a chemical facility"s security capabilities that could be exploited by terrorists. In addition, limited and controlled public disclosure of CVI is essential to protecting a companys sensitive and competitive information. Consequently, DHS protects from public disclosure CVI that facilities must develop for purposes of complying with CFATS, including documentation regarding: (1) SVAs; (2) SSPs; (3) DHSs review or approval of SVAs and SSPs; (4) ASPs; (5) inspections or audits; (6) recordkeeping requirements; (7) sensitive portions of orders, notices, or letters; (8) Top-screen or other similar documents related to tier determination; and (9) other sensitive information. In addition to what material is covered as CVI, CFATS sets forth the basic information about how to safeguard, store, and mark CVI, who is authorized to receive CVI (i.e., individuals who have a need to know to carry out chemical-facility security activities), and the sanctions that may be applied to those that disclose CVI to unauthorized personnel. n21

Before discussing compliance issues with the current DHS process for protecting CVI, it is important to note that the CVI manual is currently under re-write and that the entire area is still very much in flux. With this in mind, there are two key issues regarding the current implementation by DHS for protecting CVI that have yet to be clarified. First, the current process, if applicable to companies handling their own information, requires companies to follow two sets of similar but different (especially as they are practiced) information protection regimes Sensitive Security Information (SSI) n22 and CVI. This could create compliance issues that, in turn, would hamper companies efficient management of information, and possibly even impair security preparedness. Second, the nonregulatory requirement that all persons with access to CVI (even regarding a companys access to its own information) complete training and sign a Nondisclosure Agreement (NDA) as a prerequisite for entrance to Top-Screen is arguably overly burdensome and unnecessary. A company has a self-serving interest in protecting its sensitive information, and the enforcement provisions of CFATS ensure compliance with the CVI requirements, thereby eliminating the need for binding individuals by contract. Furthermore, the NDA requirement that an authorized user report unauthorized disclosures and security violations creates a conflict for attorneys who need to act as authorized users, but who may be limited from disclosing such information under ethical obligations. n23

G. Proposed Changes to Section 550 Preemption. Although section 550 of the DHS Appropriations Act does not contain an express preemption provision, the principle of conflict preemption maintains that state or local laws that conflict with or frustrate the purpose of a federal regulatory scheme are preempted. n24 Facilities and others may petition DHS to issue an opinion on whether particular state or local laws conflict with CFATS, in which case the federal program would preempt them. n25 However, as part of the Consolidated Appropriations Act of 2008, Congress provided additional guidance on the preemption issue by declaring that a state or political subdivision may adopt or enforce a regulation, requirement, or standard of performance regarding chemical facility security that is more stringent than the federal standard, unless there is an actual conflict. n26

III. Broader Significance

CFATS is a major homeland security development. For the first time, it imposes comprehensive federal security regulations for high-risk chemical facilities. Rather than being prescriptive (i.e., requiring that facilities take specific security measures), CFATS establishes risk-based performance standards. These risk-based standards may serve as a template for future security regulation in other industries and critical infrastructures. Consequently, corporate attorneys regardless of their business interest should monitor CFATSs implementation closely. Learning lessons from the chemical industrys experience with CFATS may save companies time and money if and when similar regulations are enacted for other industries.

Additional Information

Notice to Agricultural Facilities About Requirement To Complete Chemical Security Assessment Top Screen, *73 Fed. Reg. 1640* (Jan. 9, 2008).

Link to Chemical Security Information on the DHS Website:
http://www.dhs.gov/xprevprot/programs/gc_1169501486179.shtm.

For more information on CFATS and the preemption issue, William W. Buzbee, *Asymmetrical Regulation: Risk, Preemption, and the Floor/Ceiling Distinction*, 82 N.Y.U .L. Rev. 1547 (2007); Ross C. Paolino, *All Aboard! Making the Case for a Comprehensive Rerouting Policy to Reduce the Vulnerability of Hazardous Rail Cargoes to Terrorist Attack, 193 Mil. L. Rev. 144 (2007).*

Return to Text

n1 . Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, § 550, *120 Stat. 1355, 1388.*

n2

[2]. *72 Fed. Reg. 17688* (Apr. 9, 2007) (codified at 6 C.F.R. Part 27). *See generally* Homeland Security Deskbook § 11.05[3] (James T. O"Reilly, gen. ed. 2007).

n3

[3]. Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule, *72 Fed. Reg. 65,396-435* (Nov. 20, 2007) (codified as 6 C.F.R. Part 27, App. A).

n4

[4]. *6 C.F.R. § 27.105*.

n5

[5]. *6 C.F.R. § 27.210*.

n6

[6]. *See 6 C.F.R. § 27.205*; *72 Fed. Reg. 17,688, 17,690* (Apr. 9, 2007) (supplementary information on § 27.200(b)(2)).

n7

[7]. *6 C.F.R. § 27.105* (definition of Covered Facility or Covered Chemical Facility).

n8

[8]. *6 C.F.R. § 27.230(a)*.

n9

[9]. *See 6 C.F.R. § 27.400*.

n10

[10]. *See 72 Fed. Reg. at 65,406-10* (Nov. 20, 2007) (supplementary information).

n11

[11]. *Id.*

n12 *Nat''l Propane Gas Ass''n v. United States Dep''t of Homeland Sec., 534 F. Supp. 2d 16, 20 (D.D.C. 2008).*

n13

[13]. *73 Fed. Reg. 15,051* (notice Mar. 21, 2008).

n14

[14]. *See 6 C.F.R. § 27.200*.

n15

[15]. *6 C.F.R. § 27.230* has them.

n16

[16]. *6 C.F.R. § 27.235*.

n17

[17]. *6 U.S.C. §§ 441--444* (Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 861-865, *116 Stat. 2238); 6 C.F.R. §§ 25.1*--.10. *See generally* Homeland Security Deskbook § 8.12 (James T. O''Reilly, gen. ed. 2007).

n18

[18]. See *6 C.F.R. §§ 27.250* for inspections and audits; 27.255 for recordkeeping and appeals; and 27.400 for protection of CVI.

n19

[19]. *See 6 C.F.R. § 27.300*.

n20

[20]. *6 C.F.R. § 27.410*; *see 6 C.F.R. § 27.300*.

n21

[21]. *6 C.F.R. § 27.400*.

n22

[22]. *49 C.F.R. §§ 1520.1*-.19; Homeland Security Deskbook § 10.05[1] (James T. O"Reilly, gen. ed. 2007); *see also* Homeland Security Deskbook § 13.02 (critical infrastructure information, CII).

n23

[23]. *See 6 C.F.R. § 27.400*.

n24

[24]. *See, e.g., Maryland v. Louisiana, 451 U.S. 725, 746 (1981), cited* in *Cipollone v. Liggett Group, Inc., 505 U.S. 504, 516 (1992); MCulloch v. Maryland, 17 U.S. (4 Wheat.) 316, 427 (1819).*

n25

[25]. *6 C.F.R. § 27.405(a)*, (c).

n26

[26]. Pub. L. No. 110-161, Div. E, § 534, *121 Stat 1844, 2075 (2007).*

ABOUT THE AUTHOR(S):

Joe Whitley is a partner with the law firm Alston & Bird LLP (www.alston.com). He served as the Acting

Associate Attorney General, the third-ranking position in the Department of Justice, under President George H.W. Bush. He was appointed by Presidents Reagan and Bush, respectively, to serve as U.S. Attorney in the Middle and Northern Federal Districts of Georgia. In 2003, Mr. Whitley was appointed by President George W. Bush as the first General Counsel of the United States Department of Homeland Security (DHS), the highest ranking legal official in DHS.

Ed Britan is an associate in the Legislative & Public Policy Group in Alston & Birds (www.alston.com) Washington, D.C., office. Ed concentrates on domestic and international privacy law and the impact of federal legislation on multi-national corporations. Ed received his J.D. in 2007 from New York University School of Law. In 2003 he received a B.A. in psychology from Wesleyan University.

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.

The Western Hemisphere Travel Initiative (Land and Sea POEs) and Indian Tribes

2008 Emerging Issues 2308

The Western Hemisphere Travel Initiative and Indian Tribes: Acceptance of Tribal Documents for Entrance at Land and Sea Ports of Entry

By Tonya Davis and S. Bobo Dean

May 15, 2008

SUMMARY: Hobbs, Straus, Dean & Walker, LLP, explains what tribal documents can be used at land and sea ports of entry under Department of Homeland Security border-crossing procedures. The Western Hemisphere Travel Initiative (WHTI) final rule issued in April 2008 makes some special provisions for members of tribes U.S. and Canadian. S. Bobo Dean and Tonya Davis explain when the provisions take effect and their impact on tribes and tribal members.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Summary. The Western Hemisphere Travel Initiative (WHTI) final rule on documents required for entrance to the United States at land and sea ports of entry (POEs) n1 provides for acceptance of identification documents of federally recognized Indian tribes that are enhanced to meet the requirements of the final rule. The standard that federally recognized tribes must meet for their identification to be accepted is similar to that which states must meet for acceptance of their drivers licenses. n2 While acceptance of tribal identification cards under WHTI is a positive action, recognizing the unique relationship between the United States and tribes, concerns remain as to how WHTI requirements impact both individual privacy and tribal membership information security.

On April 3, 2008, the Departments of Homeland Security and State published in the *Federal Register* the final rule addressing documents required for entrance to the United States at land and sea ports of entry (POEs) for travel within the Western Hemisphere. This final rule implementing the Western Hemisphere Travel Initiative (WHTI) will go into effect June 1, 2009.

WHTI was mandated by the Intelligence Reform and Terrorism Prevention Act of 2004, n3 which required the Departments of Homeland Security and State to develop and implement a plan to require all travelers -- U.S. citizens and foreign nationals -- to present passports or other secure documents or combinations of documents that denote identity and citizenship when entering or re-entering the United States. WHTI establishes document requirements for travelers entering the United States who were previously exempt, including citizens of the United States, Canada, and Bermuda.

Prior to January 31, 2008, citizens of the United States and Canada could cross the mutual border with an oral declaration of citizenship and identity, n4 and U.S. citizens (but not Mexicans) could cross the border with Mexico in the same manner. An interim measure, which will remain in effect until the final rule is fully implemented on June 1, 2009, became effective on January 31, 2008. n5

The final rule tightens the number and types of documents that will be accepted as of June 1, 2009. Most notably, the final rule provides that showing a driver"s license and birth certificate as proof of citizenship and identity upon entering the United States at land and sea ports is *no longer acceptable*, except in the case of "closed loop" cruise ship voyages. n6 Otherwise, the document requirements are similar to what was proposed in the notice of proposed rulemaking, n7 with one important change for Indian tribes, namely restrictions on the acceptable types of tribal IDs.

While restricting the type of identification that can be used, the final rule acknowledges the special relationship between the United States and Indian tribes and provides for acceptance of Indian-specific identification as an alternative to a passport or passport card. Specifically, in regards to tribal identification, the final rule provides that a U.S. citizen must present a valid unexpired U.S. passport upon entering the United States but that a U.S. citizen who is a holder of a tribal document issued by a *United States qualifying tribal entity or group of United States qualifying tribal entities* n8 who is arriving from contiguous territory or adjacent islands may present the tribal document prior to entering the United States at a land or sea POE. n9

Upon full implementation of this final rule *and if designated by the Secretary of Homeland Security as acceptable under WHTI*, Native American enrollment or identification cards from a federally recognized tribe or group of federally recognized tribes will be permitted for use at entry at any land or sea POE when the bearer is arriving from contiguous territory or an adjacent island. n10 The designation by the Secretary that the tribal documentation is acceptable provides a key limitation on the tribal ID cards that will be accepted at POEs. The Secretarys designation will be contingent upon:

1. The tribe satisfactorily establishing identity and citizenship in connection with the use of its document;

2. The tribe providing DHS"s Customs and Border Protection (CBP) bureau with access to appropriate parts of its tribal enrollment records; and

3. The tribe agreeing to improve the security of its tribal documents in cooperation with CBP. n11

Until the final rule is fully implemented on June 1, 2009, unenhanced tribal enrollment documents will continue to be accepted, provided they each have a photo. n12 As of June 1, 2009, only those tribal enrollment documents that meet DHS standards will be accepted.

In addition, the final rule establishes that U.S. and Mexican Members of the Kickapoo Tribe may use their Form I-872 American Indian Cards for entry at land and sea POEs when arriving from contiguous territory and adjacent islands. Additionally, Canadian citizen members of First Nations or Bands recognized by the Canadian Government may be able to use the new Indian and Northern Affairs Canada (INAC) card issued by the Government of Canada (beginning sometime this year), containing a machine-readable zone (MRZ). The INAC card will need to be approved by the Secretary of Homeland Security, whose approval is contingent upon DHS being able to electronically verify and validate the citizenship and identity of INAC cardholders.

DHS has previously pledged to work with tribes to find low-cost ways to meet the DHS standards. As provided in *8 C.F.R. § 235.1(e)*, DHS will designate acceptable tribal ID cards as follows:

(e) *Native American Tribal Cards; alternative requirements.* Upon the designation by the Secretary of Homeland Security of a United States qualifying tribal entity document as an acceptable document to denote identity and citizenship for purposes of entering the United States, Native Americans may be permitted to present tribal cards upon entering or seeking admission to the United States according to the terms of the voluntary agreement entered between

the Secretary of Homeland Security and the tribe. The Secretary of Homeland Security will announce, by publication of a notice in the Federal Register, documents designated under this paragraph. A list of the documents designated under this paragraph will also be made available to the public.

On April 3, the same day the final rule was published in the *Federal Register*, DHS, through CBP, sent a letter to all federally recognized tribes to invite the tribes to produce an enhanced tribal document that meets WHTI requirements. n13 The document can be issued by either a tribe or a group of tribes.

A WHTI-compliant tribal identification, which DHS refers to as an Enhanced Tribal Card or ETC, will need to meet the criteria discussed above. The requirements and process for tribes developing ETCs are analogous to those of states developing WHTI-compliant IDs. n14 In particular, tribes will need to meet the same level of security requirements as a state-issued WHTI-compliant document. Washington State was the first state to produce a WHTI-compliant document. n15 The Washington State enhanced drivers license n16 includes an MRZ, a Radio Frequency Identification (RFID) chip, and a digital photograph from which biometric measurements are taken of facial features that are hard to alter (such as the size of eye sockets) and then given a numeric value that is encoded in the card. The MRZ facilitates scanning of the IDs up close, while the RFID can be read from a distance of up to around twenty feet when activated by an RFID reader. n17 The biometric measurements are intended to ensure that one person cannot obtain multiple licenses under different names. Similar technology has been in use in United States passports since 2006, although those feature a digital image of the photos provided by passport applicants, rather than a primary digital picture. n18

The types of technology used in the EDLs raise a number of questions and concerns. Some are the same as those raised and faced by the general public, such as privacy issues and the fears that unauthorized persons can read your card and that personal data will be stored or can be accessed through the card. n19 Additionally, tribes are concerned about the potential for unauthorized persons to access their membership lists and misuse the information contained therein. Additionally, some of the requirements that may seem appropriate for an enhanced state card may not be necessary or suitable for a tribal population. For instance, the population of many tribes is quite small, so using biometrics to ensure there are not duplicates in the membership database is not as necessary as it would be in a larger state population where it is not possible to know all cardholders. Similarly, the documentation of family history necessary to establish tribal membership makes some aspects of establishing tribal identification more secure than establishing state identification. Also of concern is the cost of an ETC, which CBP estimates will be about $15 per card. n20

Nonetheless, for many tribes the potential to utilize tribal identification cards at POEs is an important recognition of both their legal and political status in the United States, and an important practical matter for their members who may not be able to obtain a passport, passport card, or state EDL. n21 Those tribes interested in developing such cards within the next two years will need to contact CBP in writing by May 30, 2008. n22 This will start the process for developing ETCs. Tribes who develop ETCs will need to enter an agreement with DHS in order for the ETCs to be accepted at the land and sea POEs. Additionally, a list of accepted ETCs will be published in the *Federal Register*. n23

Practitioners in this area need to make sure their tribal clients provide written notice to the CBP of the tribes desire to develop an ETC within the next few years by the May 30, 2008, deadline. In addition, it would be wise to become familiar with the various requirements for the ETCs, the possible concerns raised by the new technologies required, and how these can be addressed for tribal clients. Development of systems that meet both DHS and tribal security concerns will be very important to ensuring that both tribal and individual information is not misappropriated and misused.

Return to Text

n1 . Documents Required for Travelers Departing From or Arriving in the United States at Sea and Land Ports-of-Entry From Within the Western Hemisphere, *73 Fed. Reg. 18,384* (Apr. 3, 2008). The final rule regarding air POEs was published at *71 Federal Register 68,412* (Nov. 24, 2006).

n2

[2]. *8 C.F.R. § 235.1(d)* and (e).

n3

[3]. Pub. L. No. 108-458, § 7209, *118 Stat. 3638* (Dec. 17, 2004).

n4

[4]. Oral Declarations No Longer Satisfactory as Evidence of Citizenship and Identity, *72 Fed. Reg. 72,744* (notice Dec. 21, 2007).

n5

[5]. The interim procedures provide for proof of citizenship and identity by presentation of either a driver"s license and birth certificate or one of the following:

. U.S. or Canadian passport

. U.S. Passport card (applications available February 1, 2008, actual cards not available until fall 2008). *See* http://www.usimmigrationsupport.org/passcard.html.

. Trusted traveler cards (NEXUS, SENTRI, or FAST)

. State or province-issued enhanced driver"s license (EDL) (when available -- this secure driver"s license will denote identity and citizenship)

. Enhanced tribal cards (when available)

. U.S. military identification with military travel orders

. U.S. Merchant Mariner Document

. Native American tribal photo identification card

. Form I-872 American Indian Card

. Indian and Northern Affairs Canada (INAC) Card.

Important Change in International Land and Sea Travel Document Procedures, *at* http://www.cbp.gov/xp/cgov/travel/vacation/ready_set_go/land_travel/chnge_in_proced.xml.

n6

[6]. A "closed loop" cruise is one in which the U.S. citizen departs from a U.S. port and returns to the same U.S. port upon completion of the voyage.

n7

[7]. *72 Fed. Reg. 35,088* (proposed June 26, 2007).

n8

[8]. A United States qualifying tribal entity is (1) a tribe, band, or other group of Native Americans (2) formally recognized by the United States Government (3) that agrees to meet WHTI document standards. *8 C.F.R. § 212.0*; *22 C.F.R § 41.0*.

n9

[9]. *8 C.F.R. § 235.1(b)(7)*; *22 C.F.R. § 53.2(b)(6)*.

n10

[10]. *See 73 Fed. Reg. at 18,397-98* (supplementary information).

n11

[11]. *Id*.

n12

[12]. Crossing U.S. Borders, *at* http://www.dhs.gov/xtrvlsec/crossingborders/index.shtm.

n13

[13]. CBP Letter of April 3, 2008, *cited in* Hobbs, Straus, Dean & Walker, LLP, report to clients on WHTI; Ensuring Successful Implementation of the Western Hemisphere Travel Initiative, *available at* http://homeland.house.gov/SiteDocuments/20080416142622-93835.pdf and http://www.cbp.gov/xp/cgov/newsroom/congressional_test/whti_implementation.xml (Joint Statement of Kathleen Kraninger, Dep. Assistant Sec"y for Policy, DHS, and Robert Jacksta, Dep. Assistant Comm"r, CBP, to Subcomm. on Border, Maritime and Global Counterterrorism, H. Comm. on Homeland Security, Apr. 16, 2008) ("We have sent out over 600 letters to all the federally recognized Native American tribes and offered to work with them toward developing a WHTI-compliant enhanced tribal document.").

n14

[14]. *See 8 C.F.R. § 235.1(d)*, (e).

n15

[15]. Other states are expected to follow. *73 Fed. Reg. at 18,404* (supplementary information at D., State Enhanced Driver"s License Projects).

n16

[16]. Information about the Washington State EDL is accessible from www.dol.wa.gov/direveslicense/edl.html and Patrick Michaels, *Enhanced Drivers" License Eases Border Crossing for Washington State Residents*, Gov"t Tech., Apr. 9, 2008, *at* www.govtech.com/gt/279970. *See generally* Enhanced Drivers Licenses: What Are They?, *at* http://www.dhs.gov/xtrvlsec/crossingborders/gc_1197575704846.shtm.

n17

[17]. Different sources give different ranges for vicinity RFID (the other type, proximity RFID, has a

shorter range).

n18

[18]. The U.S. Electronic Passport, *at* http://travel.state.gov/passport/eppt/eppt_2498.html.

n19

[19]. An Internet search on the subject of RFIDs brings up a number of stories on privacy concerns and fears regarding both the reading of the RFIDs by unauthorized persons and the ease of counterfeiting them.

n20

[20]. Based on calls and conferences with DHS. The additional price of an EDL varies from state to state: $30 in New York (https://harmonia.dmv.state.ny.us/SurveyEDL/edl-survey.htm), $15-20 in Vermont (Press Release, Governor Douglas and Homeland Security Secretary Michael Chertoff Sign MOA on Enhanced Drivers Licenses (Sept. 26, 2007), *available at* http://governor.vermont.gov/tools/index.php?topic=GovPressReleases&id=2622&v=Article); $15 in Washington (www.dol.wa.gov/driverslicens/edl.html).

n21

[21]. *See* Tonya Davis, *Implementation of the REAL ID Act and Its Effect on Tribal Sovereignty*, LexisNexis Expert Commentary (April 2008), *at* http://www.lexis.com/research/xlink?source=329925.

n22

[22]. CBP Letter of April 3, 2008, *cited in* Hobbs, Straus, Dean & Walker, LLP, report to clients on WHTI.

n23

[23]. *8 C.F.R. § 235.1(e)*.

ABOUT THE AUTHOR(S):

The law firm of Hobbs, Straus, Dean & Walker, LLP (http://www.hobbsstraus.com) is dedicated to providing high-quality legal services, including advocacy before federal, state, and local government agencies and courts, to

Indian and Alaska Native tribes and tribal organizations throughout the United States.

S. Bobo Dean is a co-founder of the firm and its managing partner. He received his undergraduate and law degrees from Yale and a B.A. and M.A. from Oxford University, where he was a Rhodes Scholar. Mr. Dean"s experience in the representation of Indian tribal governments and tribal organizations includes negotiating contracts with the Bureau of Indian Affairs and the Indian Health Service to provide services to tribal members. Mr. Dean regularly reports to tribal clients on legislative and judicial developments affecting tribal sovereignty and the Tribal Sovereignty Protection Initiative sponsored by the National Congress of American Indians. He is past chair of the Native American Concerns Committee of the Section on Individual Rights and Responsibilities of the American Bar Association.

Tonya Davis, an attorney with the firm since 2006, is a member of the Cherokee Nation of Oklahoma. Prior to entering law school, Ms. Davis worked as a legislative aide in the office of Oklahoma Congressman Mike Synar and as the Senior Policy Associate at the Center for Community Change, a Washington D.C.-based nonprofit that champions social and economic justice. Ms. Davis is a graduate of the University of Oklahoma College of Law.

16 of 19 DOCUMENTS

DHS Final Regulations on REAL ID Act Drivers' Licenses, by Whitley and Frey

2008 Emerging Issues 2214

DHS's Final Regulations Implementing Title II of the REAL ID Act of 2005, on Drivers' Licenses, by Joe Whitley and Brian D. Frey

By Joe Whitley and Brian D. Frey

April 30, 2008

SUMMARY: Joe Whitley of Alston + Bird LLP, the first General Counsel of DHS, and Brian D. Frey, also of Alston + Bird, provide an extensive discussion of the final regulations DHS issued on REAL ID drivers' licenses in early 2008. The issue of REAL ID licenses has, to put it mildly, created considerable controversy. The authors provide extensive expert advice for practitioners regarding the numerous issues raised by the regulations.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: I. Introduction

In the continuing wake of the deadly terrorist attacks of September 11, 2001, Congress passed the REAL ID Act of 2005 (the Act), n1 establishing (among other things) heightened security requirements for state identification cards accepted for official purposes by federal agencies. n2 On January 11, 2008, the Department of Homeland Security (DHS) issued implementing regulations (the Regulations) that were intended to provide the necessary practical details for implementing the basic statutory scheme. n3 This commentary is intended to highlight key requirements of the Regulations and to identify several of the most significant considerations the Regulations may raise for practitioners.

II. The Core Requirements of the Regulations

A. Timeline for State Compliance

Section 202(a)(1) of the Act originally required federal agencies to begin refusing noncompliant cards for official purposes beginning on May 11, 2008. Under the Regulations, however, this timeline has been extended. The new timeline for compliance is as follows: n4

. If a state did not file a request for extension by March 31, 2008, then enforcement would begin May 11, 2008. n5

. If a state filed for an extension by March 31, 2008, without any additional requests for extension, full compliance will be required by January 1, 2010.

. If a state filed a request for extension by March 31, 2008, and files an additional request for extension and a Material Compliance Checklist n6 by October 11, 2009, full compliance will be required by May 10, 2011.

. Any requests for extension beyond May 10, 2011, will be at the discretion of the Secretary of Homeland Security.

. Irrespective of any extensions, the Act must be enforced by December 1, 2014, for those persons younger than fifty years old by that date and by December 1, 2017, for everyone else. n7

B. Process of Issuance of REAL IDs

The Regulations also establish a variety of requirements for the issuance of REAL IDs. The primary requirements relate to the documents necessary for issuance, verification of those documents, and retention of those documents.

i. Documents Required for Issuance. For most applicants, the Regulations require that states issue REAL IDs only after obtaining: n8

. A facial photograph;

. A declaration under the penalty of perjury as to the truth of the information in the application;

. At least one document verifying identity;

. At least one document verifying date of birth;

. Proof of a Social Security number for those who have one;

. At least two documents of the states choice verifying principal place of residence;

. Evidence of lawful status in the United States.

The Regulations also allow states to define a written policy to address situations in which an individual is unable to present all of the necessary documents so long as the state makes reasonable efforts to ensure the authenticity of alternate documents used and retains copies of those documents. n9

ii. Document Verification. The Regulations require states to take a variety of steps to verify documents. These include: n10

. Making reasonable efforts to ensure the applicant does not have more than one drivers license either in a state or in more than one state;

. Verification of all documents used as proof of identity or as proof of lawful status with the issuer of the document;

. Verification of Social Security numbers with the Social Security Administration;

. Verification of birth certificates via an electronic system where available;

. Verification of documents issued by the Department of State;

. Verification of a REAL ID with the original state of issuance if it is used as an application document.

In addition, states must implement periodic training of employees to help them identify fraudulent documents. n11 Where existing systems for verification are not in place, the Regulations do not specifically provide for how states are supposed to accomplish the required verification.

iii. Document Retention. The Regulations require states to retain copies of all applications, applicant photographs, and other documents used to apply. The general retention requirements are as follows: n12

. If a state retains paper copies of documents, they must be retained for a minimum of seven years;

. If a state retains microfiche or digital copies of documents, they must be retained for a minimum of ten years.

In addition, the Regulations require each state to maintain a motor vehicle database. Each state database must include at least: n13

. All data printed on the issued card;

. The full name of the applicant;

. The applicants Social Security number;

. All of the information encoded on the common machine-readable bar code on the issued card;

. The applicants motor vehicle driving history.C. Required Physical Features of REAL IDs

The Regulations also establish specific requirements for what information and features are to be included on a REAL ID. The requirements include: n14

. Full legal name;

. Date of birth;

. Gender as determined by state law;

. Unique drivers license or identification card number that is not the applicants Social Security number

. Full facial photograph;

. Address of principal residence;

. Signature;

. Machine-readable bar code encoded with various identifying information;

. Date of transaction;

. Expiration date;

. State or territory of issuance;

. DHS-approved security marking.

Interestingly, despite the fact that the Act appeared to have been primarily intended to improve homeland security by preventing fraud in obtaining state-issued identification cards, the Regulations do not mandate many specific physical security measures that a state must implement in producing REAL IDs. Instead, DHS embraced a goal-focused

approach, requiring states to implement three levels of security features to promote detection of false cards: n15

. Level 1 security measures should use visual or tactile features to allow detection of false cards upon rapid visual inspection.

. Level 2 security features should allow detection of false cards upon examination by trained inspectors with simple equipment.

. Level 3 security features should allow detection of false cards by trained forensic specialists.

States are left to develop their own means of satisfying these levels, and must detail their proposed approach in a security plan that is submitted to DHS.

D. Security for Facilities, Materials, and Information

Recognizing the security and privacy implications of the issuance of REAL IDs and the retention of personal identification documents, the Regulations also require states to establish security plans addressing physical and digital security. A states security plan must discuss, among other things: n16

. Limits on access to facilities where REAL IDs are produced;

. Limits on access to materials used to produce REAL IDs;

. Background screening of employees;

. Reasonable administrative, technical, and physical safeguards to prevent unauthorized access, use, or dissemination of personally identifiable information.

In addition, the Regulations require states to limit use or disclosure of personally identifying information collected under the Act and the Regulations in accordance with the requirements of the Drivers Privacy Protection Act. n17 States can also opt to implement additional security and privacy measures. n18

III. Implications of the Implementing Regulations for Practitioners

The Regulations have many significant implications both for the states themselves and for individual citizens. This commentary addresses several of these implications that are likely to be among the most significant for states, state officials, legal practitioners, and their clients.

A. Time Frame for Compliance

Practitioners involved in state compliance efforts should carefully review Subpart E of the Regulations to ensure that any request for extension is timely and properly filed. n19 States that will need additional time for compliance beyond January 1, 2010, should be cognizant of the fact that material compliance is required for an additional extension. The eighteen material compliance benchmarks include: n20

. Presentation of at least one of the required source documents;

. Verification of lawful status and Social Security numbers;

. Issuance of drivers licenses or identification cards that contain integrated security features satisfying each of the three levels identified in the Regulations;

. Photographs of all applicants even if a license or identification card is not issued;

. Reasonable efforts to ensure that applicants do not have multiple licenses or multiple identities.

Given the massive state resources that will likely be required to implement the sweeping changes mandated by the Act and the Regulations, practitioners seeking to support state compliance must be vigilant as to the timing and benchmark requirements to ensure that the state has adequate time to comply.

B. Financial Implications for States

Implementing the Act and the Regulations will undoubtedly create a heavy burden for states as they attempt to work through technological and logistical requirements necessary for full compliance. n21 In recognition of this fact, as of January 2008 DHS had made $48.5 million in grant money available to states to assist with implementation costs. n22 State government practitioners should be aware of these resources and should monitor DHS releases and congressional budgets to determine whether any additional funds will be made available to support implementation.

One of the primary difficulties that states are likely to encounter during the implementation process is the technological and logistical difficulty of the document verification required by the Regulations. Apparently sensitive to this issue, DHS has explicitly reserved the right to establish alternative verification methods. n23 Thus, those involved in developing and implementing state procedures should actively monitor DHS releases in case new, less onerous methods of verification should be approved.

C. Constitutional Implications for States

The Regulations raise several constitutional concerns for states. The Tenth Amendment provides that powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States. n24 The Supreme Court has recognized that the Tenth Amendment bars the federal government from compelling states to enact and enforce federal regulatory programs. n25 State-rights advocates could argue that the Regulations violate the principles of federalism or constitute federal commandeering of the state legislatures.

Issuance of drivers licenses has historically been a state function. In contrast, immigration control and securing federal government facilities have traditionally been functions that are exclusively within the purview of the federal government. State-rights advocates may therefore argue that, by imposing limitations on state issuance of drivers licenses and forcing states to bear the cost of complying with the Act and the Regulations, the federal government has delivered an unfunded mandate to be implemented by state legislatures that interferes with matters within the states" purview.

The federal government may counter with the argument that the Act and the Regulations do not actually require state compliance. Quite the contrary, states can choose not to comply without any direct cost to the state whatsoever. Thus, the government may argue that the implementation of the Act and Regulations is a choice by states that does not implicate issues of federalism.

Ultimately, the debate over the constitutionality of the Act and the Regulations under the Tenth Amendment will be over the extent to which states are compelled to comply with the Act. n26 It is unclear whether putting states to the choice of either complying with the Act and the Regulations or having the federal government refuse to allow the states citizens to use state identification cards to access federally regulated aircraft and federal buildings rises to the level of compulsion. n27

D. Constitutional Implications for Individuals

The Regulations also implicate several constitutional considerations related to individual rights. Civil rights lawyers should consider the impact the Regulations could have on the rights to freely exercise religion, to peaceably assemble, to petition the government for redress of grievances, and to travel between the states. n28

The Regulations may implicate the First Amendment right to free exercise of religion. The Regulations require that every REAL ID contain a full facial picture of the individual. The Regulations specifically prohibit veils, scarves, and headdresses that obscure facial features or generate shadows. n29 DHS considered and ultimately rejected allowing a religious exception to this rule, preferring to allow states to continue issuing noncompliant state identification cards to affected individuals. n30 Thus, civil rights advocates may argue that, because federal agencies will not accept noncompliant state identification cards for access to federal buildings or federally regulated commercial aircraft, some individuals may be forced to choose between their right to free exercise of religion and the other constitutionally protected rights discussed below.

The Act and the Regulations may also implicate the right to travel. n31 Under the Act, noncompliant state identification cards will not be accepted for travel on federally regulated commercial aircraft, which arguably restricts an individuals right to travel. DHS counters that other documents, such as passports and military identification cards, will still be sufficient to travel. In addition, other modes of transportation are available for those who lack alternative documents. Nonetheless, the Regulations have at least some constitutional implications on the right to travel, particularly to domestic locations outside the continental United States such as the U.S. Virgin Islands or Hawaii.

Similarly, the Act and the Regulations may also have implications on the rights to freedom of assembly and to petitioning the government for redress. n32 If federal agencies deny access to federal buildings to individuals who lack REAL IDs, those without any other acceptable form of identification may be denied an opportunity to attend protests, to speak to congressional representatives, or to appear in court.

The ultimate impact of the Regulations on the constitutional rights of individuals will not become clear until enforcement begins. Nonetheless, practitioners should be aware of these and other implications of the Act and the Regulations on individual civil liberties. E. Immigration Implications

Lawyers practicing immigration law should take note of the documents required for issuance under § 37.11 of the Regulations. These requirements will apparently prevent foreign-born residents who are lawfully in the United States from obtaining REAL IDs if they do not have a passport or employment authorization documents. Thus, for example, aliens who have been granted asylum may be unable to obtain REAL IDs. In addition, the Regulations will prevent states from issuing REAL IDs to illegal immigrants. Immigration law practitioners should keep abreast of state REAL ID compliance efforts and prepare clients for the difficulties they may encounter in obtaining a REAL ID.

F. The Reissuance and Renewal Provisions

The requirements of the Act and the Regulations will likely have some effect in limiting fraudulent issuance of new licenses, given the sheer complexity of the system. One apparent shortcoming of the Regulations, however, is that, with a few minor restrictions, they permit remote reissuance and renewal of REAL IDs so long as there has been no material change in any personally identifiable information. n33 As states take steps to achieve compliance, practitioners at both the state and federal levels would be well advised to monitor proposed state policies for remote reissuance and renewal and any DHS responses thereto. In the absence of significant limitations on the reissuance and renewal process, these exceptions could easily swallow the rule and eliminate many of the intended security benefits of the Regulations.

G. Future Expansion of the REAL ID Program

The Act and the Regulations are just the beginning of what could become expansive use of the REAL ID program by the federal government. Once in force, the Act and the Regulations will require that federal agencies not accept noncompliant state identification cards for any official purposes. Official purposes include boarding federally regulated

commercial aircraft, entering federal facilities and nuclear power plants, and any other purposes that the Secretary [of Homeland Security] shall determine. n34 Thus, it is possible that the Secretary of Homeland Security or Congress will see fit to substantially expand use of the REAL ID program in the future.

Practitioners in the federal government may wish to consider alternative circumstances in which the use of REAL IDs could improve governmental efficiency and promote national security interests. A few possible instances in which a REAL ID could be exploited include: determining access to welfare or Social Security benefits, tracking citizens domestic travel, creating a more comprehensive federal do-not-fly list, restricting access to federal employment or to firearms, and hunting fugitives. In considering more expansive uses of REAL IDs, however, practitioners should be sensitive to the privacy considerations discussed below.

H. Privacy Considerations

With the efficiency and security gains that may result from implementation of the Act and the Regulations comes a variety of privacy considerations. Three of the areas that may be of concern to privacy advocates are governmental use and tracking of REAL ID information, the threat of unauthorized disclosure of personally identifying information, and possible creation of a private database containing information drawn from REAL IDs.

With the implementation of the REAL ID system, the federal government could theoretically begin tracking when, where, by whom, and for what purpose REAL IDs are used by individuals. This information could easily be consolidated into a federal database to allow the government to track the actions of U.S. citizens in any number of areas from travel history to voting patterns to involvement in anti-government political activism. This level of governmental oversight could have profound implications for the privacy of U.S. citizens vis--vis the federal government. As such, privacy advocates should closely monitor DHS regulations and congressional proposals for evidence of expansion of the REAL ID program beyond the purposes articulated in the Act and the Regulations. n35

Beyond the Orwellian, big government concerns raised by federal government monitoring of the citizenry, the Regulations pose a more immediate potential threat to citizens privacy. As discussed above, the Regulations establish new, stringent requirements for the documents that must be presented to obtain a REAL ID. n36 In addition, states will be required to maintain records of these documents and create electronic databases that include personally identifying information about the individuals to whom REAL IDs are issued. n37 These requirements will undoubtedly make state departments of motor vehicles targets for identity thieves and other nefarious individuals.

Apparently sensitive to this fact, the Regulations require states to develop security plans that include restrictions on physical access to department of motor vehicle sites as well as restrictions on electronic access to REAL ID information databases. n38 Given the formidable task of securing a massive, high-profile, digital information repository, one might have expected that the federal government itself would undertake the task of providing data security measures for electronic databases. In fact, however, the development of these security measures is left to the individual states. n39

Given this fact, those involved in state compliance efforts should consider the extent to which states may have civil exposure for accidental or intentional disclosure of personally identifying information. Similarly, private practitioners should be aware of the possibility of such disclosures and consider whether private individuals who suffer harm as a result thereof may have a cause of action against the individual perpetrator or the state itself.

Beyond the risks associated with improper disclosure of personally identifying information by state employees and criminal infiltration of the system, the Regulations create yet another privacy concern. As discussed above, REAL IDs must contain common machine-readable technology in the form of bar codes containing certain personally identifying information. n40 Because no proprietary card-reading system will be required to access this information, private parties will have little difficulty accessing such information should they choose to do so.

For example, some bars already scan a patrons drivers license to verify his or her age. n41 The Regulations leave open the possibility that such establishments could begin collecting information on their patrons via REAL IDs. n42 This information could then be used by the establishment itself for marketing purposes, or it could be sold to a third party. Thus, the Regulations leave open the possibility that the private sector could develop a massive, unregulated national database containing personally identifying information drawn from REAL IDs. State legislators should consider whether it will be necessary to implement regulations restricting private use of information on REAL IDs.

IV. Conclusion

This commentary was intended to highlight some of the more significant issues for practitioners in analyzing and applying the Regulations going forward. Practitioners should recognize that the Regulations present myriad additional issues that touch a variety of other areas of the law. Indeed, the full impact of the Act and the Regulations may not be known for quite some time as states, DHS, and Congress work toward implementation while continuing to define the ultimate scope of the use of REAL IDs. It appears likely that the Regulations will result in considerable litigation by both states and private parties. It also appears likely that Congress will seek to expand the use of REAL IDs in the future. As such, practitioners should continue to monitor the REAL ID landscape as it changes and develops. Research Links

For the most recent news on this topic, check the following database folders on lexis.com

. Mega News, US Real ID.

. Mega News, National Identity Cards.

For more information about the REAL ID Act of 2005 and its implications

. Department of Homeland Security REAL ID website, *available at* http://www.dhs.gov/xprevprot/programs/gc_1200062053842.shtm.

. Backgrounder on Drivers Licenses and the REAL ID Act, LexisNexis Expert Commentary (Dec. 2007) and sources cited.

. Tonya Davis, Implementation of the REAL ID Act and Its Effect on Tribal Sovereignty, LexisNexis Expert Commentary (Apr. 2008).

. Homeland Security Deskbook § 9.04 (James T. O"Reilly ed.) (LexisNexis Matthew Bender 2007).

. ACLU Scorecard On Final Real ID Regulations: January 17, *2008*, *available at* http://www.aclu.org/images/general/asset_upload_file162_33700.pdf, and Fuzzy Math and the Real Cost of Real ID (1/16/2008), *available at* http://www.aclu.org/safefree/general/33690res20080116.html.

. Center for Democracy and Technology, REAL ID: What Should Congress Do Now?: CDT Analysis of the REAL ID Act and the Department of Homeland Securitys Final Regulations, *available at* http://www.cdt.org/security/identity/20080201_REAL%20ID_hillbrief.pdf.

Return to Text

n1 . Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, Pub. L. No. 109-13, div. B, *119 Stat. 231* (May 11, 2005).

n2

[2]. *See generally 49 U.S.C. § 30301* note. Title II is the relevant part of the law; the rest deals with immigration and border control.

n3

[3]. *73 Fed. Reg. 5272* (Jan. 29, 2008) (to be codified at 6 C.F.R. pt. 37).

n4

[4]. 6 C.F.R. §§ 37.5(b)-(c), 37.63.

n5

[5]. DHS granted all the states and territories extensions. Press Release, DHS, All Jurisdictions Meet Initial REAL ID Requirements (Apr. 2, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1207167055742.shtm.

n6

[6]. *See* Material Compliance Checklist, Appendix A to the regulation but not in the *Federal Register.* It is reproduced from the version of the regulation first released by DHS before publication in the *Federal Register*.

n7

[7]. *6 C.F.R. § 37.5(b)*-(c).

n8

[8]. *6 C.F.R. § 37.11*.

n9

[9]. *6 C.F.R. § 37.11*. Note that the Regulations also provide an exception for REAL IDs issued in support of Federal, State, or local criminal justice agencies or other programs that require special licensing or identification to safeguard persons or in support of their official duties. *6 C.F.R. § 37.11(i)*.

n10

[10]. *6 C.F.R. § 37.13*.

n11

[11]. *6 C.F.R. § 37.41(b)(5)*.

n12

[12]. *6 C.F.R. § 37.31*.

n13

[13]. *6 C.F.R. § 37.33*.

n14

[14]. *6 C.F.R. §§ 37.17, 37.19*.

n15

[15]. *6 C.F.R. § 37.15*.

n16

[16]. *6 C.F.R. §§ 37.41*, *37.43*.

n17

[17]. *6 C.F.R. § 37.41(b)(2)(iii)*. *See generally 18 U.S.C. §§ 2721* to *2725* (discussing the purposes for which state departments of motor vehicles may release personally identifying information, including, for example, use by state or federal law enforcement).

n18

[18]. *6 C.F.R. § 37.41(b)(2)(iii)*.

n19

[19]. 6 C.F.R. §§ 37.5137.71.

n20

[20]. *See* Material Compliance Checklist at the end of this commentary.

n21

[21]. DHS has estimated that the total cost of implementing the final rule, including costs to states and individuals, could be as much as $9.9 billion. *73 Fed. Reg. 5272*, *5324-29* (Jan. 29, 2008) (supplementary information). In 2006, the National Governors Association, National Conference of State Legislatures, and American Association of Motor Vehicle Administrators issued a "National Impact Analysis" of the REAL ID Act"s cost and other implementation issues. The analysis is at http://www.aamva.org/aamva/DocumentDisplay.aspx?id=%7b055B37F6-E619-4ACE-AAEC-10CC9F79CB1A%7d.

n22

[22]. *See* Press Release, DHS, DHS Increases Funding for REAL ID Grant Program and Extends Applications Deadline (Jan. 29, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1201630837774.shtm.

n23

[23]. *6 C.F.R. § 37.15*.

n24

[24]. U.S. Const. amend. X.

n25

[25]. *See, e.g., New York v. United States, 505 U.S. 144, 161 (1992).*

n26

[26]. *Id.*

n27

[27]. *Compare id.* (holding that a federal law requiring states to take title to radioactive waste violated the Tenth Amendment) *with South Dakota v. Dole, 483 U.S. 203 (1987)* (holding that a federal law making ten percent of state highway funding contingent on the state enacting a minimum drinking age of twenty-one did not violate the Tenth Amendment because pressure on states to comply did not rise to the level of compulsion).

n28

[28]. U.S. Const. amend. I; *see also id. at art. IV, § 2, cl. 1*.

n29

[29]. *6 C.F.R. § 37.17*.

n30

[30]. *73 Fed. Reg. 5272, 5301* (Jan. 29, 2008) (supplementary information).

n31

[31]. *See generally* U.S. Const. art. IV, § 2, cl. 1 (addressing limitations on the authority of states to restrict the right to travel between the states); *Zemel v. Rusk, 381 U.S. 1 (1965)* (discussing the right to travel vis--vis the federal government).

n32

[32]. U.S. Const. amend. I.

n33

[33]. *6 C.F.R. §§ 37.23, 37.25*.

n34

[34]. REAL ID Act § 201(3), *49 U.S.C. § 30301* note.

n35

[35]. *See, e.g.*, Anne Broache, *DHS: Real ID could help shut down meth labs* (Jan. 16, 2008), *at* http://www.news.com/8301-10784_3-9851813-7.html*; see* Press Release, Coalition for a Secure Driver"s License (CSDL), Drug Free America Foundation, and the Association of Community Employment Programs for the Homeless (A.C.E.) Endorse DHS Final Regulations for the REAL ID Act (Jan. 11, 2008), *available in* PR Newswire database on lexis.com.

n36

[36]. *6 C.F.R. § 37.11*.

n37

[37]. *6 C.F.R. § 37.13*.

n38

[38]. *6 C.F.R. § 37.41*.

n39

[39]. *Id.*

n40

[40]. *6 C.F.R. § 37.19*.

n41

[41]. *See, e.g.*, Robert Schwaneberg, *Bars" harvesting of personal data spurs hearings on privacy laws*, Star-Ledger (Newark, N.J.), Jan. 23, 2007, at 16; Ian T. Shearn, *License scanning is illegal, state says*, Star-Ledger (Newark, N.J.), Nov. 23, 2006, at 41; Ian T. Shearn, *With ID swipe, Big Brother bellies up to the bar*, Star-Ledger (Newark, N.J.), Nov. 21, 2006, at 1.

n42

[42]. *See 73 Fed. Reg. 5272, 5292, 5306* (Jan. 29, 2008) (supplementary information).

ABOUT THE AUTHOR(S):

Joe Whitley is a partner in the Washington, D.C., office of Alston & Bird LLP (www.alston.com). Joe had an extensive career in the Department of Justice. In the George H.W. Bush administration, Joe served as the Acting Associate Attorney General, the third-ranking position in the Department of Justice. He was appointed by Presidents Reagan and Bush, respectively, to serve as U.S. Attorney in the Middle and Northern Districts of Georgia. Throughout his career, Joe served under five United States Attorneys General in a number of key operational and policy positions.

In 2003, Joe was appointed by the President as the first General Counsel of the United States Department of Homeland Security (DHS), the highest ranking legal official in DHS. He held that position for two years before his departure and return to private practice.

Joe is the former leader of Alston & Birds Government Investigations and Compliance Group. He has successfully represented numerous individuals and corporations in major government investigations throughout the United States and internationally. While Joe continues to devote part of his practice to white-collar defense and compliance, he is also the head of the firms Global Security and Enforcement Team. In this capacity, Joe deals with a broad range of homeland

security issues, including customs and immigration enforcement matters.

Brian D. Frey is an associate in the Washington, D.C., office of Alston & Bird LLP (www.alston.com), where he is a member of the firms Litigation and Trial Practice group. Brians practice is primarily focused on government and internal investigations and general civil litigation. Brian received his J.D., magna cum laude, from Georgetown University Law Center, where he was a member of the Georgetown Law Review staff. He received his B.A., magna cum laude, from the University of Notre Dame.

17 of 19 DOCUMENTS

Implementation of the REAL ID Act and Its Effect on Tribal Sovereignty

2008 Emerging Issues 2127

Hobbs, Straus, Dean & Walker, LLP on Implementation of the REAL ID Act and Its Effect on Tribal Sovereignty

By Tonya Davis

April 15, 2008

SUMMARY: Tonya Davis of Hobbs, Straus, Dean & Walker, LLP, discusses problems with the final rule DHS issued in January 2008 to implement the provisions of the REAL ID Act of 2005 (Pub. L. No. 109-13, div. B) regarding drivers' licenses. The regulation, at *73 Fed. Reg. 5271* (codified at 6 C.F.R. Part 37), causes many concerns for Native Americans. The author lays out the regulation's practical and procedural problems, as well as potential remedies.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: Cite as: Davis, Tonya, Implementation of the REAL ID Act and Its Effect on Tribal Sovereignty. LexisNexis Expert Commentary, *(Insert date you accessed the document online)*.

The final regulation n1 implementing the REAL ID Act n2 drivers' license provisions n3 prevents States from accepting tribal ID cards as forms of identification, and ignores the problems many tribal members will face in obtaining required documents. DHS refused to adhere to the directive of Executive Order 13,175, n4 requiring consultation and coordination with Indian tribal governments in the development of federal policies that have tribal impact, in developing the REAL ID final regulations. However, even absent an administrative fix by DHS, there are still opportunities to reduce the restrictive effect of the REAL ID regulations on tribes.

On January 11, 2008, DHS released its final regulations (final rule) under the REAL ID Act of 2005. The REAL ID Act requires people entering federal buildings, boarding airplanes, or entering nuclear power plants to present identification that has met certain security and authentication standards. n5 These standards involve a number of aspects of the process used to issue identification documents, including: information and security features that must be incorporated into each card; application information to establish the identity and immigration status of an applicant before a card can be issued; and physical security standards for facilities where drivers' licenses and applicable identification cards are produced. n6

The REAL ID Act has caused considerable concern amongst many, including a number of States that have protested its imposition upon them, n7 and some States refused to comply and have backed up that refusal, going so far as to not apply for the extensions mentioned in note 5. n8 However, while REAL ID has the potential to cause problems for many Americans, including inconveniences for travelers from noncompliant states, the Act poses more than just a mere inconvenience to tribal governments and tribal members.

The overarching concern expressed by many tribal governments and advocates is that the imposition of the REAL ID rule, without formal consultation and without recognition of the fact that members of federally recognized Indian tribes have a viable means of identifying who they are through a tribal ID, was a violation of the federal government's government-to-government relationship with tribes (as well as the Executive Orders that require federal agencies to consult with tribes on federal regulations). n9 This is troubling because DHS has the potential to affect many aspects of tribal life, particularly for tribes located along the international border or with traditional or cultural sites in Canada or Mexico.

The government-to-government consultation process is one of the key mechanisms by which the federal government shows its respect for tribal sovereignty and the right of tribes to self-govern. The consultation process was implemented as an effort to recognize the need of Indian tribes to have significant and meaningful input on the federal policies that affect their members and their manner of governing. Refusal to consult is indicative of a lack of understanding of the role tribal governments play in their members' lives, and of how modern tribes function. In many cases tribes function similarly to state governments, issuing car tags, licenses, and identification to their citizens, as well as providing cultural, economic, and government services to their members.

The promulgation of the REAL ID regulations without consultation is thus problematic from a procedural point of view, as well as a practical one. The final rule contains several provisions that are troubling to Indian tribes and their members. This reflects the lack of consultation and has real potential to harm tribal governments and members as a result.

The restriction on acceptance of REAL ID-compliant state identification may prove an impediment to tribal governments seeking to exercise their right to a government-to-government relationship with the federal government. Many tribes see the requirement of a State-issued identification card as an assault on tribal sovereignty. But even for those willing to obtain a state identification card, REAL ID is an impediment. This impediment is realized three ways:

(1) If the tribal member is from a REAL ID-noncompliant state (for example, Montana, which has a significant Native population, is saying it will not comply) and thus unable to obtain REAL ID from the State, yet also unable to have tribal identification be REAL ID-acceptable, it will be difficult for that tribal member to enter a federal facility or travel to Washington by air to pursue a relationship with the federal government;

(2) The requirements of REAL ID may, as many fear, make it more difficult to use currently acceptable forms of identification, such as tribal identification, for travel or to enter federal buildings; and

(3) If a tribal member in a REAL ID-compliant state wants to obtain a State-issued driver's license or identification, the REAL ID regulations restrict what documents can be used to verify identity, preventing tribal members from using their tribal IDs -- the documents most readily available to the majority of tribal members. Native Americans from States that have previously accepted tribal identification cards or Bureau of Indian Affairs identification cards will, under REAL ID, no longer be able to use those cards to verify identity.

Take the situation of an Indian elder who does not have a State-issued birth certificate or a passport n10 as an example. In the past, in many states with a large American Indian population (such as Oklahoma), that elder would have been able to use her Tribal Identification Card to obtain a state identification card or driver's license. n11 However, the REAL ID regulations specifically prevent States from accepting tribal IDs as proof of identity. n12

Suppose that same elder needs to visit a federal facility (perhaps to obtain a copy of her Social Security card, or to visit her congressman). She probably n13 would not have a REAL ID because she does not have a birth certificate, and most likely, the federal facility will not accept her tribal ID card as identification. n14 She would find it very difficult to enter the facility.

In response to comments on these same matters, DHS has asserted that it received assurances from the Department of the Interior and the Bureau of Indian Affairs (BIA) that "Tribal members are similarly situated to the general

population and have access to the identification documents set forth in the rule." n15 However, the BIA, tribal leaders, and other advocates have communicated to DHS that this is often not the case, particularly in regard to elderly Indians and Indians who live in remote areas, many of whom do not have the State-issued birth certificates required under the regulations to obtain REAL ID, let alone passports.

While other Americans may be similarly situated in terms of lacking birth certificates or passports (the documents generally necessary to prove identity under REAL ID), the unique role of Indian tribes in the United States and the government-to-government relationship between tribes and the federal government make the imposition of these new requirements on State-issued identification particularly onerous for tribal governments. For those tribes that issue their own identification cards, the final rule makes no provision for using tribal identification either as an acceptable form of REAL ID or as a basis to obtain a REAL ID-compliant state license. The proscription on accepting tribal identification ignores the fact that requirements to obtain a tribal ID are far more stringent than state processes. Indeed, tribal membership processes, which include proving lineage back several generations n16 and presentation of this proof to an enrollment committee, make it all but impossible for nonmembers to obtain tribal identification.

DHS representatives have stressed that the REAL ID Act does not govern what federal agencies can accept for allowing entry to federal facilities. n17 Presumably, however, the Transportation Safety Administration, a DHS agency that governs airport security, will follow the REAL ID restrictions stringently and will be less likely to accept alternative identification if State-issued drivers' licenses cannot be used. n18

While under the REAL ID Act DHS does not have the authority to tell federal agencies what alternative forms of ID they may accept, many fear that the restrictions in REAL ID will be replicated in other areas. The REAL ID regulations -- whether they have the authority to do so or not -- may well lead other agencies to be more restrictive as to identification than they have been in the past. Indeed, the Bureau of Indian Affairs, as recently as February 29, 2008, could not assure tribes it could accept tribal IDs after the REAL ID implementation date. n19

For those who are concerned about the REAL ID regulations and their effect on tribes, there are a number of steps that can be taken to mitigate the harm caused by REAL ID.

First, make sure the State or States the tribe in question is located in apply for extensions for compliance. This will allow additional time to seek fixes to the problems caused by REAL ID before it goes into effect. n20

Second, encourage federal agencies and commercial airlines to accept tribal identification as an alternate form of identification.

Third, encourage state governments to accept tribal documents. As suggested by the REAL ID regulations, "Where a Tribal member does not have the necessary document to establish identity, date of birth, or lawful status, a States exception process can take this into account based on the States knowledge and experience with Tribal documents in its area of jurisdiction." n21

The aforementioned are short-term solutions that can help to mitigate the effect of REAL ID on tribal members. More long-term solutions include supporting a legislative fix that would allow the use of tribal IDs, and encouraging DHS to address the problem administratively. And, of course, it is very important to encourage education of DHS officials regarding the federal government's tribal consultation policy, and to ensure that they comply in the future.

Return to Text

n1 . Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule, *73 Fed. Reg. 5271* (Jan. 29, 2008) (to be codified at 6 C.F.R. Part 37).

n2

[2]. Div. B, Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, Pub. L. No. 109-13, *119 Stat. 231* (May 11, 2005).

n3

[3]. Backgrounder on Drivers' Licenses and the REAL ID Act, LexisNexis Expert Commentary (Dec. 2007).

n4

[4]. Consultation and Coordination With Indian Tribal Governments (Nov. 6, 2000), *65 Fed. Reg. 67,249* (Nov. 9, 2000).

n5

[5]. All fifty states, the District of Columbia, Puerto Rico, and the U.S. territories obtained extensions of the original May 11, 2008, deadline for compliance. Press Release, DHS, All Jurisdictions Meet Initial REAL ID Requirements (Apr. 2, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1207167055742.shtm. Had they not obtained extensions, federal agencies would not accept their drivers' licenses or identification cards for official purposes ("official purpose is defined under § 201 of the Act to include access to federal facilities, boarding of federally regulated commercial aircraft, entry into nuclear power plants, and other purposes established by the Secretary of Homeland Security). Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule, *73 Fed. Reg. 5271* (Jan. 29, 2008) (to be codified at 6 C.F.R. Part 37). States were required to seek extensions from DHS by March 31, 2008. These extensions will expire on December 31, 2009, unless a State requests an additional extension no later than October 11, 2009 (with a certification that the State has achieved the benchmarks set forth in the Material Compliance Checklist). Final rule at 5272 (supplementary information). As of May 11, 2011, drivers' licenses and identification cards will not be accepted from States that are not in full compliance with the provisions of REAL ID, meaning that the State has begun issuing REAL ID-compliant identification. *Id.*

n6 . Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule, *73 Fed. Reg. 5271* (Jan. 29, 2008) (to be codified at 6 C.F.R. Part 37).

n7 . In recognition of the burden on States, the deadlines to have REAL ID-compliant licenses and ID cards have been staggered based on age. For those under fifty as of December 1, 2014, federal agencies will not accept

driver's licenses or identification cards for official purposes unless DHS has determined that the issuing State is in compliance with the final rule (Subparts A through D) and the card presented by the individual meets the standards of the rule. For those born on or after December 1, 2014, the deadline to be REAL ID-compliant is December 1, 2017. Final rule at 5272 (supplementary information).

n8

[8]. DHS treated Montana's letter of protest as a request for an extension. Governor Schweitzer of Montana commented, "We sent them a horse. If they choose to call it a zebra, that is their business." Devlin Barrett, *Chertoff: ID Must Comply to Fly*, AP, Mar. 21, 2008, at http://ap.google.com/article/ALeqM5hGWEcbtYTTl9RTiO3YS_POnaYJ9gD8VI70FG1.

n9

[9]. *See, e.g*., Executive Order 13,175; *see also* George W. Bush, Memorandum on Government-to-Government Relationship with Tribal Governments (Sept. 23, 2004), in Public Papers of the Presidents (Sept. 27, 2004), and *available at* http://www.epa.gov/tribal/pdf/president-bush-2004.pdf.

n10

[10]. Note that the requirements to obtain a passport can be onerous for similar reasons, and the additional factor of cost (about $100 for a basic adult passport) makes it unlikely passports will be a viable alternative. *See* http://travel.state.gov/
passport/get/fees/fees_837.html.

n11

[11]. *See* http://www.dmv.org/ok-oklahoma/id-cards.php.

n12

[12]. *See* final rule at 5333 (*6 C.F.R. § 37.11*).

n13

[13]. DHS explains that "the final rule permits a State to use its exceptions process to determine what alternative documents an individual may present in this limited circumstance to establish his or her date of

birth." Final rule at 5294 (supplementary information). But is certainly would be better to have another option that is not part of the "exceptions process," even if that process may work for the particular individual.

n14

[14]. If the facility currently accepts tribal ID, it can continue to do so, or if the facility requires no ID it can continue to do so; however, many are concerned that REAL ID will have a ripple effect and federal facilities will begin to restrict what documentation they accept.

n15

[15]. See final rule at 5294-95 (supplementary information).

n16

[16]. Tribal membership often requires the ability to trace ancestry back to a tribal roll, such as the Dawes Rolls, or proof of a quantum of Indian blood, which is often certified by the Bureau of Indian Affairs through a Certificate of Degree of Indian Blood (CDIB) card.

n17

[17]. See note 14.

n18

[18]. Currently, those who lack a government-issued ID must provide two alternate forms of identification and/or go through additional screening. It is not clear what those who have a driver's license from a noncompliant State will be required to do under the final rule, although the final rule comments note significant delays will be likely. *See* final rule at 5273 (supplementary information).

n19

[19]. BIA officials spoke in a conference call with tribal leaders about REAL ID. Their comments are discussed in a memorandum to clients from Hobbs, Strauss, Dean & Walker LLP, *Developments Impacting Tribal Sovereignty* (Mar. 7, 2008).

n20

[20]. See *supra* note 5 for information on extensions.

n21

[21]. Final rule at 5295 (supplementary information).

ABOUT THE AUTHOR(S):

The law firm of Hobbs, Straus, Dean & Walker, LLP (http://www.hsdwlaw.com) is dedicated to providing high-quality legal services, including advocacy before federal, state, and local government agencies and courts, to Indian and Alaska Native tribes and tribal organizations throughout the United States. **Tonya Davis**, an attorney with the firm since 2006, is a member of the Cherokee Nation of Oklahoma. Prior to entering law school, Ms. Davis worked as a legislative aide in the office of Oklahoma Congressman Mike Synar and as the Senior Policy Associate at the Center for Community Change, a Washington D.C.-based nonprofit that champions social and economic justice. Ms. Davis is a graduate of the University of Oklahoma College of Law.

18 of 19 DOCUMENTS

Background Explanation of Various Terrorist Lists

2008 Emerging Issues 1545

Background Explanation of Various Terrorist Lists

By Backgrounder

December 17, 2007

SUMMARY: Confused by the different lists? So are many people. Here is a concise explanation of the Foreign Terrorist Organizations List, the Terrorist Exclusion List, the Specially Designated Terrorists List, the Specially Designated Global Terrorist List, and others. Some involve blocked assets and trouble for anyone dealing with a person or entity on the list; some "merely" prevent someone from entering the United States; and some can involve civil penalites and even criminal punishment. So it's important that you -- and your clients -- understand what these lists are.

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

ARTICLE: In all the talk currently about security checks, people may be confused about the different lists mentioned. Is the Foreign Terrorist Organizations list what airlines (and soon ships n1) check passenger names against? No, they check against the Terrorist Screening Center's Terrorist Watchlist n2 -- which would include members of FTOs.

What are the No-Fly and Selectee lists? Are they different? No, they are pieces of the Terrorist Watchlist. n3 People on the No-Fly list are not to be allowed to fly. Selectees are to receive additional screening.

The courts lately have been seeing many, many cases involving name checks for people applying for citizenship or lawful permanent resident status. n4 Is the name check the same thing? Not really. The FBI name check includes a check of the person's fingerprints and criminal record, as well as a database that may overlap the Terrorist Watchlist, n5 but the idea is to see whether the person is of good enough character. In other words, more than associations with terrorism is involved.

How about the Terrorist Exclusion List? That also is different. As the Congressional Research Service explained in 2003, n6

the Executive branch maintains an intricate array of lists pursuant to various legislation and Executive Orders. These lists do overlap; however, the Executive Branch implements sanctions against state sponsors of terrorism, terrorist organizations, and individual terrorists somewhat differently, depending upon which legislation applies, what the purpose is, and which list is being considered. There are also international lists .

Or as it also put it,

The FTO list is often confused with some of the other 'terrorist lists' that are maintained by the U.S. government. These include the 'state-sponsors of terrorism' list, which is pursuant to Section 6(j) of the 1979 Export Administration Act (P.L. 96-72; *50 U.S.C. app. 2405*(6)(j)); the 'Specially Designated Terrorists' (SDTs) list, which is pursuant to the International Emergency Economic Powers Act (P.L. 95-223; *50 U.S.C. 1701* et seq.) and was initiated in 1995 under Presidential Executive Order 12947; the 'Specially Designated Global Terrorists' (SDGT) list, initiated in 2001 under Presidential Executive Order 13224; and, finally, the 'Specially Designated Nationals and Blocked Persons' (SDN) list, a master list that contains the other lists. All of these are summarized and maintained by the Office of Foreign Assets Control of the Treasury Department. Lastly, the 'Terrorist Exclusion List' or 'TEL,' which relates to immigration and is pursuant to Section 411 of the USA P[ATRIOT] Act of 2001 (*8 U.S.C. 1182*) is maintained by the State Department. Like the FTO list, the TEL includes the names of terrorist organizations, but it has a broader standard for inclusion, is subject to less stringent administrative requirements, and is not challengeable in court. There is a complicated interplay among all of these lists, and it is important to distinguish them from the better-known FTO list. n7

There are easy ways to check the lists: Lexis.com's Office of Foreign Assets Control Database says it contains

the U.S. Department of the Treasury's master list of Specially Designated Global Terrorists and entities with Blocked Persons, U.S. Department of Commerce Bureau of Export Administration Denied Persons List, FBI Fugitives 10 Most Wanted, Most Wanted Terrorist, United Nations Sanction list, World Bank of Debarred Firms list, Politically Exposed Persons, Commodity Futures Trading Commission, Office of Comptroller of Currency list of Unauthorized Banks, Interpol European Union Most Wanted, Bank of England and a FinCEN [U.S. Department of the Treasury's Financial Crimes Enforcement Network] Special Alert List.

Additionally, the Code of Federal Regulations n8 contains an "Alphabetical Listing of Blocked Persons, Specially Designated Nationals, Specially Designated Terrorists, Specially Designated Global Terrorists, Foreign Terrorist Organizations, and Specially Designated Narcotics Traffickers," and the Department of the Treasury keeps the Specially Designated Nationals list, which combines the lists of Specially Designated Terrorists, Specially Designated Global Terrorists, and State Sponsors of Terrorism, at http://www.treasury.gov/offices/enforcement/ofac/sdn (last visited December 15, 2007).

But what are these lists about?

Start with the "State Sponsors of Terrorism." They are what they sound like: countries that, according to the Secretary of State, have repeatedly provided support for acts of international terrorism. n9 The five countries are Cuba, Iran, North Korea, Sudan, and Syria. Designation means restrictions on exports and foreign aid to them, and financial restrictions. People dealing with them can be sanctioned under section 6(j)(1)(A) of the Export Administration Act of 1979, n10 section 620A of the Foreign Assistance Act of 1961, n11 or section 40(d) of the Arms Export Control Act. n12

"Foreign Terrorist Organizations" n13 are designated by the Secretary of State according to Immigration and Nationality Act § 219. n14 The Secretary consults with and may be acting on the recommendation of the Attorney General or Secretary of Homeland Security, or both. Congress can review and reject the designation. Once the designation is published in the *Federal Register*, the organization may seek judicial review.

The criteria n15 are that the organization be foreign, engage in terrorist activity n16 or terrorism, n17 or continue to have the capacity and intent to do so, and threaten the security of U.S. nationals or U.S. national security. It is illegal to give material support or resources n18 to an FTO. Any non-U.S. citizen who is a representative or member of an FTO is inadmissible to the United States (and, therefore, also removable if he or she made it in). Furthermore, U.S. financial institutions must freeze and report any FTO assets.

The other big list is the Terrorist Exclusion List, n19 which stems from USA PATRIOT Act n20 § 411(a). n21 The Secretary of State, in consultation with or on the recommendation of the Attorney General or Secretary of

Homeland Security, or both, names organizations that have committed terrorism or incited terrorist activity in circumstances indicating intentions to cause death or other serious bodily injury, or that prepare, plan, or provide material support for terrorist activity, or that gather information on potential targets of terrorist activity. Supporters and associates of designated organizations are inadmissible.

The Specially Designated Terrorists list began as a measure against individuals and entities trying to disrupt the Middle East peace process. The authority comes from the International Emergency Economic Powers Act. n22 After September 11, 2001, the President used Executive Order 13,224 n23 to block the property and property interests of a list of terrorists and people and entities that materially supported them, originating the Specially Designated Global Terrorists list. Both lists are maintained and supplemented by the Secretary of the Treasury. Assets of any person or entity on the list will be frozen by the Secretary. n24

The Department of the Treasury lists about two dozen current or defunct sanctions programs, only one of which is called Anti-Terrorism. n25 As the Department points out, n26 though, much of the designation activity comes from Executive Order 13,224, which President Bush signed on September 23, 2001. The consequences of designation under 13,224 are blocked (or frozen) property, prohibitions on contributions to or for designees, and civil and criminal penalties for attempts at or actual evasion.

For more information, see

31 C.F.R. Ch. V, especially *31 C.F.R. § 594.101* to Ch. V, App. B.

Steve C. Posner, Privacy Law and the USA PATRIOT Act chs. 3 and 5.

U.S. Department of State Related Links page at http://www.state.gov/e/eeb/c9985.htm (last visited Dec. 15, 2007).

Return to Text

n1 . *72 Fed. Reg. 48,320* (Aug. 23, 2007); *see also* 72 Fed, Reg. 53,394 (proposed Sept. 18, 2007) (private aircraft).

n2

[2]. *Watching the Watch List: Building an Effective Terrorist Screening System, Hearing Before the S. Comm. on Homeland Security and Governmental Affairs, 110th Cong., Oct. 24, 2007 (statement of Paul Rosenzweig, DHS Deputy Assistant Secretary for Policy).*

n3

[3]. *Id.*

n4

[4]. *See, e.g., Sinha v. Upchurch, 2007 U.S. Dist. LEXIS 90286* (N.D. Ohio Dec. 7, 2007); *Saleem v. Keisler, 2007 U.S. Dist. LEXIS 80044* (W.D. Wis. Oct. 26, 2007).

n5

[5]. For more on the various databases that could be involved in security checks, see Steve C. Posner, Privacy Law and the USA PATRIOT Act § 6.28.

n6

[6]. Audrey Kurth Cronin, Congressional Research Service, Order Code RL32120, The FTO List and Congress: Sanctioning Designated Foreign Terrorist Organizations, at CRS-5 (Oct. 21, 2003).

n7

[7]. *Id.* at Summary page.

n8

[8]. 31 C.F.R. Ch. V, App. A.

n9

[9]. State Sponsors of Terrorism, at http://www.state.gov/s/ct/c14151.htm (last visited Dec. 15, 2007).

n10

[10]. *50 U.S.C. App. § 2405(j)(1)(A).*

n11

[11]. *22 U.S.C. § 2371*.

n12

[12]. *22 U.S.C. § 2780(d)*.

n13

[13]. *See generally* Cronin, *supra* note 6; Fact Sheet, U.S. Dep't of State Office of Counterterrorism, Foreign Terrorist Organizations (FTOs) (Oct. 11, 2005), *available at* http://www.state.gov/s/ct/rls/fs/37191.htm (last visited Dec. 15, 2007).

n14

[14]. *8 U.S.C. § 1189*; Margaret D. Stock, *Providing Material Support to a Foreign Terrorist Organization: The Pentagon, the Department of State, the People's Mujahedin of Iran, & The Global War on Terrorism*, 11 Bender's Immigr. Bull. 521 (June 1, 2006).

n15

[15]. Fact Sheet, *supra* note 13.

n16

[16]. As defined by INA § 212(a)(3)(B), *8 U.S.C. § 1182(a)(3)(B)*, which Margaret Stock has pointed out is so broad that about the only thing that might be excluded is politically motivated fist-fighting. Stock, *supra* note 14, at 523.

n17

[17]. As defined in *22 U.S.C. § 2656f(d)(2)* as premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents.

n18

[18]. *18 U.S.C. § 2339A(b)* defines this as, basically, providing any property or service.

n19

[19]. Fact Sheet, U.S. Dep't of State Office of Counterterrorism, Terrorist Exclusion List (Dec. 29, 2004), *available at* http://www.state.gov/s/ct/rls/fs/2004/32678.htm (last visited Dec. 15, 2007).

n20

[20]. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, *115 Stat. 272 (2001).* LexisNexis has a database of USA PATRIOT Act materials. *See generally* Steve C. Posner, Privacy Law and the USA PATRIOT Act Appendix A.

n21

[21]. Steve C. Posner, Privacy Law and the USA PATRIOT Act, App. A [USA PATRIOT Act] Sec. 411.

n22

[22]. *50 U.S.C. §§ 1701--1707*.

n23

[23]. Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism, *66 Fed. Reg. 49,079* (Sept. 25, 2001).

n24

[24]. Cronin, *supra* note 6, at CRS-4.

n25

[25]. The list of sanctions programs is at http://www.treasury.gov/offices/enforcement/ofac/programs/ (last visited Dec. 15, 2007).

n26

[26]. Designations, at http://www.treasury.gov/offices/enforcement/designations.shtml (last visited Dec. 15, 2007).

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

ABOUT THE AUTHOR(S):
A LexisNexis Backgrounder.

19 of 19 DOCUMENTS

Cooney of Venable, LLP, on Doe v. Gonzales

2008 Emerging Issues 507

Cooney of Venable, LLP, on Doe v. Gonzales

By John F. Cooney

September 20, 2007

SUMMARY: John F. Cooney on National Security Letter Provisions of USA PATRIOT Act Being Struck Down by Southern District of New YorkIn Doe v. Gonzales, Judge Marrero of the Southern District of New York struck down provisions of the Electronic Communication Privacy Act, as amended by the USA PATRIOT Act, Pub. L. No. 107-56, *115 Stat. 272 (2001),* the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, *120 Stat. 192 (2006),* and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, 109 Pub. L. No. 178, *120 Stat. 278.* The provisions struck down, *18 U.S.C. §§2709*(c), 3511(b), related to nondisclosure orders directed to electronic communication service providers (ECSPs) and judicial review of the nondisclosure orders. The orders accompany national security letters (NSLs). The court held that the provisions violated principles of First Amendment law and the separation of powers. This commentary, written by John F. Cooney of Venable LLP, a distinguished litigator who has worked on national security issues as an Assistant to the Solicitor General and Deputy General Counsel to the Office of Management and Budget and in private practice, critiques and analyzes this decision in relation to other First Amendment cases.

PDF LINK: Click Here for Enhanced PDF of Commentary

ARTICLE: *Doe v. Gonzales* n1 involves a constitutional challenge under the First Amendment and the principle of separation of powers to provisions of the USA PATRIOT Act that authorize the Federal Bureau of Investigation to issue an order to an individual electronic communication service provider ("ECSP") directing that it may not disclose to any person, including its customer, that the ECSP has received a National Security Letter ("NSL") obliging it to provide the government with records concerning a subscriber and his telephone or Internet activity.

The U.S. District Court for the Southern District of New York (Judge Marrero) found the mechanism for issuing nondisclosure orders to be unconstitutional and issued an injunction banning the government from issuing NSLs to ECSPs. The court stayed its order for ninety days to permit the government to seek relief from the Second Circuit.

The validity of the procedures under which nondisclosure orders are issued likely will be resolved by the Supreme Court, unless Congress amends the statute while an appeal is pending. Congress previously amended the ECSP mechanism in response to an earlier District Court ruling that the original provisions violated the First and Fourth Amendments. n2 Further legislative action probably will be required to address at least some of the constitutional deficiencies identified by the District Court.

Constitutional Challenges. The USA PATRIOT Act n3 authorizes the FBI to issue to wire and electronic communications providers an NSL compelling production of records concerning a subscriber's communications. Section 2709(c) further provides that on a case-by-case basis the FBI may, without prior judicial review, issue an accompanying order that prohibits the recipient from disclosing to any person that the agency has sought access to information through an NSL, upon the FBI's certification that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."

A related judicial-review provision n4 provides that an ECSP may challenge a nondisclosure order and that a reviewing court may modify or set aside the order if it determines that "there is no reason to believe" that disclosure "may endanger the national security of the United States [or] interfere with a criminal, counterterrorism or counterintelligence investigation . . . . " Further, if the Department of Justice "certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations," the court is required to treat that certification "as conclusive unless the court finds that the certification was made in bad faith."

An unidentified Internet service provider and the ACLU brought a facial challenge to the constitutionality of these statutes. The plaintiffs also challenged § 2709(c) insofar as it authorizes the FBI to issue a nondisclosure order based on a determination that disclosure of receipt of the NSL would endanger "national security," on the ground that this term is so broad as to give the FBI unfettered discretion to suppress constitutionally protected speech. They further challenged the constitutionality of § 3511(d)-(e), which provide for the closure of hearings and sealing of records in these proceedings to prevent disclosure of an NSL request and authorize ex parte, in camera judicial review of government submissions that contain classified information.

The Court's Decision. The District Court held that §§ 2709(c)(1) and 3511(b) violate the First Amendment and the principle of separation of powers. It rejected plaintiffs' challenges to the term "national security" and the confidentiality procedures applicable to judicial review of challenges to nondisclosure orders.

(1) The First Amendment Violation. The court held that § 2709(c)(1) constitutes an unconstitutional prior restraint of the ECSP's ability to speak about its receipt of an NSL. Relying on First Amendment cases dealing with obscenity and adult entertainment, especially *Freedman v. Maryland*, n5 the court found that the NSL provisions must satisfy three procedural requirements: (a) expeditious judicial review must be available; (b) any restraint prior to judicial review must be brief; and (c) the government must bear the burdens of initiating judicial review and, once in court, of justifying the prior restraint. The court held that the first two requirements were satisfied, but that § 2709(c) was unconstitutional because it did not require that the government initiate the court proceeding to review the nondisclosure order and that the government bear the burden of proof that the prior restraint was justified on national security grounds.

(2) The Violation of Separation of Powers. The court held that § 3511(b) constitutes an unconstitutional intrusion by the legislative branch into the authority of the judicial branch to determine the standard under which the constitutionality of a statute is assessed. The court concluded that the standard of review prescribed in § 3511(b) -- that a nondisclosure order may be set aside only if the court "finds that there is no reason to believe that disclosure may endanger the national security," and requiring a finding of "bad faith" to overturn a Justice certification that disclosure may jeopardize national security -- is sharply at odds with the principles that the Supreme Court has established to determine the constitutionality under the First Amendment of a law imposing prior restraints. The court did not rely on an obvious, related point, that the "no reason to believe" standard shifts the burden of proof to the challenger and essentially requires it to prove a negative.

(3) The Inseverability Determination. The court held that the unconstitutional provisions governing nondisclosure orders were inseverable from the substantive provisions of § 2709(a)-(b) authorizing the issuance of NSLs. The court therefore enjoined the FBI from issuing NSLs to ECSPs, even if the demands for documents are not accompanied by nondisclosure orders.

Analysis of the Decision. The court's decision appears correct on several crucial issues: (a) the First Amendment

requires adequate procedural safeguards for reviewing prior restraints, including appropriate time constraints within which the government's actions can be challenged in court; n6 (b) prior restraints are presumptively unconstitutional, and the government bears the burden of proving that the prohibition on speech is justified by a compelling government interest; n7 (c) the judicial procedure as a whole must satisfy due process requirements; and (d) Congress cannot adopt a rule of decision for resolution of constitutional challenges to a law that does not provide at least the minimum degree of protection required by prior Supreme Court decisions. n8

One aspect of the court's decision appears problematic -- its conclusion that prior First Amendment decisions require that, in every case in which a nondisclosure order is issued, the government initiate a judicial proceeding to have the order sustained, regardless of whether the ECSP has notified the government that it does not wish to contest the restriction.

The court addressed the question of what procedures are required in a case involving national security by incorporating wholesale the procedures that the Supreme Court had adopted in *Freedman* to assess the validity of prior restraints in the obscenity context. There are two problems with this approach.

First, the application of the strict scrutiny standard will be substantially different in a case concerning regulation of adult entertainment and a case in which the government interest advanced to defend a restraint on speech is the concern with protecting the physical safety of the country and its population. The government has a compelling interest in preventing the risk to national security that could occur if a potential terrorism suspect were informed that he was being investigated. For example, the German government recently was forced to take down earlier than it wished an al-Qaeda related group that was plotting to attack a U.S. airbase, because a policeman disclosed to a member of the group during a traffic stop that he was on a national watch list.

Second, the Supreme Court has not found that all three *Freedman* factors must be followed even in the context of regulation of adult entertainment. As the District Court noted, in a 1990 decision reviewing a city licensing scheme that imposed a prior restraint on sexually oriented businesses engaged in constitutionally protected activity, five members of the Court did not require the government to initiate a court proceeding to deny a license. n9 Further, there are other prior-restraint contexts, such as the denial of a parade permit, in which the frustrated speaker is required to initiate judicial proceedings to vindicate its First Amendment rights, even though the government bears the ultimate burden of proof on the merits.

Unlike in the obscenity context, a requirement that the government institute a judicial confirmation proceeding each time an ECSP nondisclosure order is issued would appear to present substantial national-security related concerns for both the executive agencies and the courts. Further, alternative procedures would appear to be available that would address these government concerns while protecting the First Amendment rights of recipients.

The government's concerns arise from the fact that it likely would have to submit national security-related information in its court papers in order to present a prima facie case for sustaining the nondisclosure order. The executive agencies would have to make a risk-based decision about how much national security information should be set forth in a document that would be outside their control. Further, the courts would need to adopt protective procedures commensurate with the sensitivity of the national security information submitted. These concerns prompted Congress to adopt the procedures in § 3511(d)-(e), which the court upheld, anticipating that the government's principal pleadings would be filed under seal, that the proceedings would have be closed to the public, and that much of the evidence submitted to meet the governments burden of proof would be classified and would be appropriately reviewed ex parte and in camera.

There are no publicly available data concerning how many NSLs have been issued to ECSPs or how many letters were accompanied by nondisclosure orders. As the court found, the empirical evidence shows only that NSL recipients generally have little or no incentive to challenge nondisclosure orders. The public data suggest that only two challenges have been made in federal court since the original enactment of the [Electronic Communication Privacy Act] statute in

1986.

Under these circumstances, the government would have a reasonable argument that it should not be required to initiate and pursue a confirmation proceeding for every nondisclosure order that is issued, in view of the incremental risk, however small, that sensitive national security information might inadvertently be compromised in such a case and in view of experience, which shows that few recipients of nondisclosure orders have demonstrated interest in challenging them.

Alternative techniques appear to be available that would not require the government to initiate a confirmation proceeding and present a prima facie case for nondisclosure orders in situations in which an ECSP does not wish to challenge the prohibition, but would fully protect the First Amendment rights of any recipient that does in fact wish to challenge such an order. For example, § 3511(b) could be amended to provide that the government must institute a proceeding to confirm a nondisclosure order in cases where an ECSP notifies the government that it does wish to be able to discuss its receipt of the NSL; and that upon submission of such a notification, the order would lapse automatically unless the government filed the required court action within a short, defined period.

Many other procedures are available through which the conflicting interests could be accommodated. In each case, the threshold question for the courts would appear to be whether, in the national security context as in some other areas involving prior restraints, the recipient may constitutionally be required to take some step to trigger judicial review of the government action, or whether the government must in every case initiate a court action to sustain the constraint.

From Supreme Court decisions in other contexts in which the government prohibits individuals from disclosing confidential information, the indispensable requirements of the First Amendment appear to be that the person so constrained have a full opportunity to challenge the nondisclosure order, if he wishes; that any proceeding to confirm the order be conducted on an accelerated schedule; and that the government carry what the Supreme Court described in the Pentagon Papers case as a "heavy burden" of showing justification for the imposition of a prior restraint. n10

Finally, since district courts are ill-equipped to handle the classified information that the government must submit to sustain its burden of proof, Congress should amend the law to provide for review of challenges to nondisclosure orders by a centralized court such as the Foreign Intelligence Surveillance Act court n11 that has appropriate security safeguards. Centralized review also would provide for consideration of these challenges by judges who are familiar with the national security issues involved and would promote consistency in decisions.

Return to Text

n1 . *2007 U.S. Dist. LEXIS 65879* (S.D.N.Y. Sept. 6, 2007).

n2 . *Doe v. Ashcroft, 334 F. Supp.2d 471 (S.D.N.Y. 2004).*

n3 . The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, §505(a), *115 Stat. 272.* This was codified at *18 U.S.C. § 2709* and amended by the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §116(a), *120 Stat. 192 (2006),* and the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, 109 Pub. L. No. 178, §4(b), *120 Stat. 278.*

n4 . *18 U.S.C. § 3511 (b).*

n5 . *380 U.S. 51 (1965).*

n6 . *See FW/PBS, Inc. v. City of Dallas, 493 U.S. 215 (1990).*

n7 . *United States v. Aguilar, 515 U.S. 593, 605 (1995)* (the government may not generally restrict individuals from disclosing information that lawfully comes into their hands, in the absence of a state interest of the highest order); *New York Times, Inc. v. United States, 403 U.S. 713, 714 (1971)* (even in national security cases, the government carries a "heavy burden" of showing justification for the imposition of a prior restraint).

n8 . *See Dickerson v. United States, 530 U.S. 428 (2000)* (holding unconstitutional statute that permitted introduction at trial of confessions that do not satisfy the constitutionally based *Miranda* requirements); *Robertson v. Seattle Audubon Society, 503 U.S. 429 (1992)* (separation of powers principles apply to congressional determination of standard of review).

n9 . *FW/PBS, 493 U.S. at 229-230* (OConnor, J., plurality opinion), 246 (White, J., dissenting).

n10 . *New York Times, 403 U.S. at 714* .

n11 . Described in *50 U.S.C. § 1803.*

ABOUT THE AUTHOR(S):

John F. Cooney is a partner at Venable LLP (www.venable.com) in Washington, D.C. He received his A.B. degree in 1970 from Brown University and his law degree in 1973 from the University of Chicago. He frequently litigates separation of powers and other constitutional issues in trial and appellate courts. He previously served as an Assistant to the Solicitor General in the Department of Justice and as Deputy General Counsel of the Office of Management and Budget, where he worked extensively on national security and separation of powers issues as part of the White House review process. Among the cases in which he has been involved are: Jackson v. Birmingham Board of Education, 544 U.S. 167 Shepardize (2005) (application of Title IX of Civil Rights Act to retaliation claims); Dickerson v. United States, 530 U.S. 428 Shepardize (2000) (striking down statute that purported to overrule the Miranda decision); National Credit Union Administration v. First National Bank, 522 U.S. 479 Shepardize (1998) (field of membership of credit unions); Bowsher v. Synar, 478 U.S. 714 Shepardize (1986) (striking down Gramm-Rudman law on separation of powers grounds); Chlorine Chemistry Council v. EPA, 206 F.3d 1286 Shepardize (D.C. Cir. 2000) (non-zero threshold for carcinogen under Safe Drinking Water Act); Mova Pharmaceutical Corp. v. Shalala, 140 F.3d 1060 Shepardize (D.C. Cir. 1998) (removing obstacles to marketing generic drugs); and United States v. Credit Lyonnais, C.D. Cal., Crim. No. 03-760 (representing the French Republic in criminal prosecution of one of its instrumentalities).