

SUPPLEMENT TO REPORT ON UNITED STATES FEDERAL LAWS REGARDING PRIVACY AND PERSONAL DATA AND APPLICATION TO BIOMETRICS

The following is an update to the 2004 Report of the National Biometric Security Project on United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics (the “Report”). This supplement reports on eight new privacy initiatives that have appeared since the original report and updates five key areas reviewed in the original report. New topics are: (1) Homeland Security Presidential Directive #12 (HSPD-12); (2) The Western Hemisphere Travel Initiative (WHTI); (3) The Registered Traveler (RT) program; (4) State Laws Regarding Biometric Information in Schools; (5) Laws requiring DNA from Convicts and Arrestees; (6) The DHS Automated Targeting System (ATS); (7) The Traveler Redress Inquiry Program (TRIP); and (8) Revisions to Federal Rules of Civil Procedure addressing privacy.

Updates include: (1) Judicial Interpretation of the Term “record” under the Privacy Act of 1974; (2) The Privacy cases against the airlines; (3) the US-VISIT Program; (4) CAPPs II and the new Secure Flight Program; and (5) The Real ID Act.

Attached to this Supplement is an Appendix of pending and recently passed legislation impacting privacy and the use of biometrics.

New Privacy Initiatives Since the Original Report

1. *National Security Presidential Directive 59/Homeland Security Presidential Directive 24*

NSPD 59/HSPD 24 is the first Presidential Directive to deal exclusively with biometrics—more specifically, their application to identification and screening to enhance national security. The purpose of the framework is to “ensure that Federal executive department agencies...use [interoperable] methods and procedures in the collection, storage, use, analysis, and sharing on biometric and associated biographic and contextual information of individuals...”¹ Biometrics will be used by various federal agencies to screen for “known and suspected terrorists (KSTs)”—with the information on those individuals being collected, stored and shared to prevent terrorist acts.

The Directive also promotes greater inter-agency flow of biometric information by requiring agencies to “make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security.” The sharing, though, must respect applicable confidentiality and privacy laws. These new policies are to be implemented by the assistant to the president for Homeland Security and Counter terrorism, the assistant to the

¹ The White House Office of the Press Secretary, “National Security Presidential Directive and Homeland Security Presidential Directive,” <http://www.whitehouse.gov/news/releases/2008/06/20080605-8.html>.

president for National Security Affairs and the Director of the Office of Science and Technology.²

2. Homeland Security Presidential Directive #12 (HSPD-12)

HSPD-12 promulgated a program designed to create a single standard for identification for all federal government employees and contractors by use of a “smart card”. These smart cards will allow for identification with photographic images printed on the card, and biometric data, PINs, and other electronic credentials (such as digital certificates) stored on the card. The overall goal of HSPD-12 is to increase security, reduce identity fraud, protect the personal privacy of the cardholder, and generally achieve appropriate security assurance by verifying the identity of individuals seeking physical access to government facilities and electronic access to government information systems.³ HSPD-12 initially required agencies, at a minimum, to issue standards-compliant personal identity verification (PIV) card to all new employees and contractors by October 27, 2006. This date has been extended to October 2008.

With respect to the biometric data to be stored on the smart cards, NIST released Special Publication 800-53, Revision 1 (Final Public Draft), *Recommended Security Controls for Federal Information Systems* for a four-week public comment period, which ended on November 17, 2006.⁴ It specifies technical acquisition and formatting requirements for the biometric credentials of the smart cards and “enumerates required procedures and formats for fingerprints, fingerprint templates, and facial images by appropriate instantiation of values and practices generically laid out in published biometric standards.”⁵ According to NIST, fingerprints were chosen as the biometric for the smart card “because fingerprints are the least invasive and most cost-effective, reliable, repeatable, and accurate means of verification available using public[ly] available technology.”⁶ In addition to the two fingerprints that will be stored on the cards, an electronic facial image may be used, but is not required. However, a photograph of the cardholder is required to be printed on the card for visual inspection and verification. The cardholder’s name and the expiration date of the card will also be printed on the card. No other personal information, such as Social Security number, address, or telephone number, is required to be stored on the card. The release of the stored biometric information occurs only after the cardholder provides the correct PIN.⁷

Implementation of HSPD-12 is moving forward. Federal agencies, including the Department of Commerce, USDA, NASA, and the US General Services Administration appear to be attempting to comply with the October 2008 deadline as their websites offer instructions to employees for obtaining the required identification cards and training schedules on how to use them.

² Ibid.

³ <http://www.osec.doc.gov/osy/HSPD12/HSPD-12Information.htm>

⁴ <http://csrc.nist.gov/publications/drafts.html>.

⁵ <http://crypto-world.info/news/index.php?prispevek=2672&sekce=s>.

⁶ <http://www.itl.nist.gov/lab/bulletns/bltnmar05.htm>.

⁷ *Id.*

3. The Western Hemisphere Travel Initiative (WHTI)

The WHTI is a border crossing program that will allow US citizens to pass through land and sea ports of entry between the United States, Canada, Mexico, the Caribbean, and Bermuda using a card (known as a “Passport Card” or “PASS Card”) containing a “vicinity-read radio frequency identification” (RFID) chip linked to government databases. As part of the initiative, US citizens were required to present a passport when traveling back into the United States by air beginning on January 23, 2007.⁸ Although biometric information is not currently being used in these cards, it is possible that biometric information will be included in the future. One of the concerns about using RFID technology is that a person not enrolled in the program could borrow or steal someone else’s card to get across the border. There is also concern that hackers could obtain the information stored on the card by simply coming within close enough range of one, a process known as “digital pick-pocketing.”⁹

The Passport Card was developed by the US Department of State and is a less expensive option for people who don’t require a full passport. The Passport Card may be used instead of a passport at US land and sea ports-of-entry by travelers arriving from Canada, Mexico, the Caribbean, and Bermuda. However, the passport card may not be used for air travel.

The Department of State began accepting applications for the Passport Card on February 1, 2008¹⁰, and began production of the U.S. Passport Card in July 2008.¹¹

As of January 31, 2008, Canadian and US citizens need to present WHTI-compliant documentation or government-issued identification and proof of citizenship in order to cross the US-Canadian border. This requirement will be extended to require most US citizens entering the United States by land or sea to have a passport, Passport Card, or a “trusted traveler” card, such as NEXUS, FAST, or SENTRI (these programs are discussed below).¹²

NEXUS, FAST, and SENTRI are “trusted traveler” programs approved under the Western Hemisphere Travel Initiative designed to expedite land border crossings between the United States and Mexico and the United States and Canada for frequent travelers. SENTRI stands for Secure Electronic Network for Travelers Rapid Inspection and was first implemented for land crossings in 1995 and now includes 15 lanes in nine ports of entry along the United States-Mexico border.¹³ NEXUS permits travelers who have been pre-qualified by both US Customs and Border Protection and the Canada Border Services Agency to cross the United States-Canada border easily. NEXUS can be used at land crossings, but is unique in that it also permits

⁸ http://travel.state.gov/travel/cbpmc/cbpmc_2223.html.

⁹ “U.S. Biometric Entry Card Program On Track” May 10, 2006. http://www.ibia.org/biometrics/industrynews_view.asp?id=448

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.*

¹³ http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/sentri_fact.ctt/sentri_fact.pdf.

holders to use it at sea crossings and, most importantly, airports.¹⁴ FAST (Free And Secure Trade), is an initiative geared toward expediting the process for clearing commercial shipments at the border. Commercial drivers who frequently cross either the northern or southern United States border may submit applications and, if approved, are permitted expedited entry into the United States with their cargo.¹⁵

The State of Washington began issuing “enhanced driver licenses” that contain RFID technology that lawmakers hope may be used as an alternative to a passport or pass card when re-entering the United States at land or sea ports-of-entry.¹⁶ DHS has encouraged states to enter into agreements with it to issue these enhanced driver licenses to their citizens to facilitate border crossings.¹⁷

4. The Registered Traveler (RT) Program

The RT program currently being deployed by the Transportation Security Administration (TSA) in conjunction with private industry is intended to provide expedited security screening for select airline passengers who voluntarily submit certain biometric and biographical information to a TSA-approved vendor, successfully complete a security threat assessment, and pay an enrollment fee.¹⁸ Only US citizens, US nationals, and lawful permanent residents are eligible to participate, and all participants must be over the age of 12.¹⁹

Also known as the Registered Traveler Interoperability Pilot, the program is currently in operation for some carriers operating out of John F. Kennedy Airport and LaGuardia Airport, Albany International Airport, the Denver International Airport, the Indianapolis International Airport, the Jacksonville International Airport, the Little Rock National Airport, the Norman Y. Mineta San Jose Airport, Orlando International Airport, the Reno/Tahoe International Airport, the San Francisco International Airport, Newark Liberty International Airport, the Cincinnati/Northern Kentucky International Airport, Washington Dulles International Airport, Oakland International Airport, Ronald Reagan Washington National Airport, and Westchester County Airport.²⁰

Under this program, private companies, in conjunction with TSA, permit individuals to pay a “membership” fee and undergo a TSA-administered security threat assessment in advance, thus permitting members to undergo curtailed security screening at airports.²¹ Travelers who wish to participate in this program must submit fingerprints and iris images during the enrollment

¹⁴ http://www.cbp.gov/xp/cgov/travel/trusted_traveler/nexus_prog/nexus.xml.

¹⁵

http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/fast/fast_ref_guide.ctt/fast_ref_guide.pdf.

¹⁶ <http://www.rfidjournal.com/article/articleprint/3066/-/1/>.

¹⁷ http://www.dhs.gov/xnews/releases/pr_1196872524298.shtm.

¹⁸ Overview of the Registered Traveler Program from the TSA website: www.tsa.gov. TSA estimates that the enrollment fee will be around \$30. However, private companies selling the services to the public are expected to charge more.

¹⁹ From the Registered Traveler Program Model issued by TSA in May 2006.

²⁰ <http://www.tsa.gov/approach/rt/index.shtm>.

²¹ http://www.tsa.gov/what_we_do/rt/rt-travelers.shtm.

process and security threat assessment phase. Only portions of these biometric images are stored on the card so that the original image cannot be recreated from the information on the card.^{22 23}

The Registered Traveler program offers dedicated lanes at certain airports to minimize waiting times for members.²⁴ The program is available to US citizens, permanent resident aliens, and US nationals.²⁵ Private companies administering programs include FLO (administered by The FLO Corporation),²⁶ CLEAR (administered by Verified Identity Pass),²⁷ and RtGo (operated by Unisys Corporation)²⁸. The annual fee for these programs ranges from \$100 to \$128 and includes a \$28 fee charged by TSA.

In connection with the Registered Traveler Program, TSA has published a draft set of documents for companies in the private industry who will be sponsoring the program entitled Security, Privacy, and Compliance Standards for Sponsoring Entities and Service Providers. In drafting these standards, TSA researched applicable existing guidance and government regulations relating to privacy and information security, conducted a vulnerability assessment of the program, and considered standards from other public-private partnership programs. Companies desiring to participate in the program must submit an application to TSA. Once accepted, enrollment providers will be required to establish a written privacy policy governing the data collected. This privacy policy must be provided to every individual participant. TSA has also published a Privacy Impact Assessment of the program in order to provide the public with an outline of how the biometric and biographical information is collected, processed, and protected.²⁹

The biometric data that will be required include a digital photograph and flat fingerprint images of all fingers. The enrollee will also have the option of submitting two iris images as a supplementary biometric for use in identity verification. The enrollee will then select either the fingerprints or the iris images as the primary biometric of preference for use in identity verification at the security kiosk. In addition to the biometric data, a photograph of the enrollee is displayed on the outside of the enrollee's Registered Traveler card and may be used to assist the verification provider in ensuring that the cardholder is a Registered Traveler participant. However, the photograph may not be used as a substitute for the biometric information.

5. State Laws Regarding Schools Collecting Biometric Information from Students

For several years, schools around the world, including schools in the United Kingdom, Belgium, France, and Italy, have obtained biometric information from their students to identify their students for services such as checking out library books and paying for lunches.^{30 31 32 33}

²² http://www.rtgocard.com/faq.htm#How_are_my_fingerprints_and_iris_image_biometrics_used.

²³ http://www.tsa.gov/assets/pdf/pia_tsa-rt_20060901.pdf.

²⁴ *Id.*

²⁵ http://www.tsa.gov/what_we_do/rt/rt-travelers.shtm.

²⁶ <http://www.flocard.com>.

²⁷ <http://www.flyclear.com>.

²⁸ <http://www.rtgocard.com>.

²⁹ *Id.* (Overview of the Registered Traveler Program from the TSA website: www.tsa.gov).

³⁰ <http://www.privacyinternational.org/survey/phr2003/countries/unitedkingdom.htm>.

³¹ <http://www.dataprotection.ie/viewprint.asp?DocID=409&m=f>.

Some schools in the United States have also been implementing biometric systems with mixed reactions from students and parents. Schools in states such as Minnesota³⁴, South Carolina³⁵, Arizona³⁶, and Illinois have used biometric identification systems, with varying success. The University of Georgia has been using hand geometry biometrics for 36 years, and the first hand geometry system that was installed in the University of Georgia dining hall in 1972 to verify meal plan participants has since grown to a fully integrated solution that secures three different types of facilities on the school's extensive campus. Continued use of hand geometry in the dining hall, the system was expanded to include student housing – to verify a student lives in the building – and to the student recreational center – to verify membership in the sports facility. [See BTAM V2.]

In Illinois, a parent was concerned that her children were unable to have school lunches because the children refused to submit a finger scan as part of the payment process. Her lobbying prompted State Representative Bob Pritchard and State Senator Kim Lightford to introduce bills requiring school districts to: (1) adopt a policy meeting certain criteria before collecting biometric information from their students; (2) prohibit the sale or disclosure of student biometric information; (3) and require parental consent before obtaining biometric information from students³⁷. This bill was signed into law on August 1, 2007³⁸.

In addition to establishing policy standards, the Illinois law restricts the use of biometrics in schools, but notably does not completely prohibit it. The Arizona State Senate is considering a bill to completely outlaw the use of fingerprints in schools.³⁹ There are two other states that forbid the use of fingerprints: Michigan law prohibits all governmental agencies, including public schools, from fingerprinting children, except in certain circumstances,⁴⁰ and Iowa law currently prohibits the use of fingerprints in schools. Interestingly, and representative of the temporal nature of statutory law, in Iowa, the State Department of Education is now requesting that lawmakers revisit their earlier decision and begin permitting fingerprint scanners in schools again⁴¹.

Although, as reflected above, there is some resistance to the idea, the trend seems to be that using fingerprints to identify students is becoming more widespread. A complete bar to using fingerprints in schools appears to be the exception rather than the rule: most states appear to be comfortable with using biometrics in schools as long as parents are notified and an opt-out method exists.

³² <http://www.enseignons.be/actualites/2007/02/06/empreintes-digitales-pour-securer-l-ecole/>.

³³ <http://www.pcinpact.com/actu/news/31010-Empreintes-digitales-pour-les-enfants-dune-e.htm>.

³⁴ <http://www.eschoolnews.com/news/top-news/index.cfm?i=32174&CFID=4580932&CFTOKEN=46539411>.

³⁵ <http://www.cbn.com/CBNnews/52958.aspx>.

³⁶ <http://hsdailywire.com/single.php?id=5437>.

³⁷ <http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0232&print=true&write=>.

³⁸ <http://www.eff.org/deeplinks/2007/09/victory-against-school-biometrics-illinois>.

³⁹ <http://hsdailywire.com/single.php?id=5437>.

⁴⁰ <http://www.ag.state.mi.us/opinion/datafiles/2000s/op10144.htm>.

⁴¹ <http://www.desmoinesregister.com/apps/pbcs.dll/article?AID=/20080128/NEWS10/801280330>.

6. Laws requiring DNA Samples from Convicts and Arrestees

The federal DNA Analysis Backlog Elimination Act of 2000⁴² (the “DNA Act”) requires individuals convicted of certain crimes and incarcerated or on parole, probation, or supervised release to submit a DNA sample. The DNA Act withstood judicial scrutiny in 2004 in United States of America v. Thomas Cameron Kincade⁴³. Typically, requiring a DNA sample from an individual would violate the right against unreasonable searches and seizures found in the Fourth Amendment.⁴⁴ However, the United States Supreme Court has found that searches in three categories⁴⁵ are exempt from the warrant and probable cause requirements: (1) “exempted areas”, including searches at border crossings⁴⁶, in prisons⁴⁷, and at airports⁴⁸; (2) administrative searches, including inspections of closely-regulated businesses⁴⁹ and other routine regulatory investigations⁵⁰; and (3) special needs searches, including in schools⁵¹ and roadside checkpoints⁵². In Kincade, the Ninth Circuit found that requiring a DNA sample from individuals not in the prison system was permitted under the Fourth Amendment.

The DNA Act was amended in 2004 to expand the qualifying crimes to all felonies. In 2007, the United States Court of Appeals for the Ninth Circuit found the amended DNA Act was also constitutional in United States of America v. Thomas Edward Kriesel, Jr.⁵³ The Ninth Circuit held that, because of his status as a supervised releasee from prison, Mr. Kriesel had a “diminished expectation of privacy in his own identity specifically, and tracking his identity is the primary consequence of DNA collection.”⁵⁴

In its opinion, the Ninth Circuit highlighted that every circuit to consider a challenge to the DNA Act has found that collecting DNA from nonviolent felons does not violate the Fourth Amendment under either a “totality of the circumstances” test (used by a majority of the circuits) or a “special needs” test (used by the Second and Seventh Circuits)⁵⁵ while the Sixth Circuit upheld the DNA Act using both tests⁵⁶.

⁴² Public Law No. 106-546, 114 Stat. 2726 (2000).

⁴³ 379 F.3d 813 (9th Cir. 2004). The Kincade holding was discussed in detail in the initial Privacy Report, pp. 38-39.

⁴⁴ U.S. CONST. amend. IV.

⁴⁵ A discussion of these three categories is set out in Kincade at 822-24.

⁴⁶ See United States v. Ramsey, 431 U.S. 606 (1977); United States v. Flores-Montano, 541 U.S. 149 (2004); United States v. Montoya de Hernandez, 473 U.S. 531 (1985).

⁴⁷ See Hudson v. Palmer, 468 U.S. 517 (1983).

⁴⁸ See Chandler v. Miller, 520 U.S. 305 (1997); United States v. Edwards, 498 F.2d 496 (2d Cir. 1974).

⁴⁹ See New York v. Burger, 482 U.S. 691 (1987); United States v. Biswell, 406 U.S. 311 (1972).

⁵⁰ See Camara v. Mun. Ct. of S.F., 387 U.S. 523 (1967).

⁵¹ See Bd. of Educ. v. Earls, 536 U.S. 822 (2002); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995).

⁵² See Illinois v. Lidster, 540 U.S. 419 (2004).

⁵³ 508 F.3d 941 (9th Cir. 2007).

⁵⁴ *Id.* at 947.

⁵⁵ *Id.* at 946.

⁵⁶ *Id.*

In addition to the DNA Act passed by Congress, as of January 2008, 44 states have enacted state laws mirroring the DNA Act that require at least some convicted felons to provide a DNA sample.⁵⁷ Several states have expanded the scope of the federal law. Nine states have passed laws requiring samples from people convicted of certain misdemeanors, typically sex offense or child victim misdemeanors. Eleven states have laws requiring samples from certain arrestees, i.e., even before conviction.⁵⁸ Many of these laws are several years old and appear to have withstood judicial challenges. For example, the Louisiana law requiring DNA samples from arrestees was passed in 1997 and became effective in 1999.⁵⁹ The Texas law passed and became effective in 2001.⁶⁰ The Virginia law dates back to 2002.⁶¹

The Supreme Court of New Jersey decided two companion cases⁶² in 2007 challenging the constitutionality of the New Jersey DNA Database and Databank Act of 1994 (the “NJ Act”),⁶³ as amended. The New Jersey Supreme Court found the NJ Act to be constitutional as applied to adults and juveniles under both the United States Constitution and the New Jersey Constitution, and further found the NJ Act withstood both the balancing test approach⁶⁴ and the more stringent “special needs” analysis. The balancing test examines the situation to determine how much the search intrudes on an individual’s privacy and balances that intrusion against the legitimate government interest in performing the search. The special needs exception arises when “special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.”⁶⁵ In the O’Hagen case, the special need was the need to obtain identification information that could “be used in the event independent evidence demonstrates that a crime has been committed.”⁶⁶ The New Jersey Supreme Court found that DNA test results were similar to photographs and fingerprints and therefore useful in solving other crimes. The Court held that DNA test results could be stored and used to solve crimes committed prior to the taking of the DNA sample without violating constitutional search and seizure restrictions.⁶⁷

The DNA Act and similar state laws permit DNA samples to be taken from individuals and analyzed. The results of these analyses are included in the Combined DNA Index System (“CODIS”), a centrally managed database run by the FBI with access to DNA samples collected by federal, state, and local crime laboratories and programs.

7. DHS Automated Targeting System (ATS)

In November 2006, DHS gave notice in the Federal Register of the existence of the Automated Targeting System (“ATS”).⁶⁸ ATS was reported as being created in the 1990s by the

⁵⁷ <http://www.ncsl.org/programs/cj/dnadatabanks.htm>.

⁵⁸ *Id.*

⁵⁹ La. R.S. § 15:609.

⁶⁰ Tex. Gov’t Code § 411.1471.

⁶¹ Va. Code Ann. § 19.2-310.2:1.

⁶² State of New Jersey v. O’Hagen, 189 N.J. 140 (N.J. 2007) and A.A. v. Attorney General of New Jersey, 189 N.J. 128 (N.J. 2007).

⁶³ N.J.S.A. § 53:1-20.17-20.28

⁶⁴ Please see our discussion of the balancing test in the initial Privacy Report, p. 40.

⁶⁵ Skinner v. Ry. Labor Executives’ Ass’n, 489 U.S. 602, 619 (1989).

⁶⁶ O’Hagen, at 146.

⁶⁷ A.A., at 140.

⁶⁸ <http://edocket.access.gpo.gov/2006/06-9026.htm>.

US Customs Service (the precursor to US Customs and Border Protection) to screen shipping cargo, but the program was not made public. ATS is used by DHS and US Customs and Border Protection to assign ratings or “risk assessments” to all travelers, including US citizens, entering and leaving the United States. Part of ATS’s purpose, as stated in the Federal Register, is “to perform targeting of individuals, including passengers and crew, focusing [U.S Customs and Border Protection] resources by identifying persons who may pose a risk to border security, may be a terrorist or suspected terrorist, or may otherwise be engaged in activity in violation of US law”.⁶⁹

ATS does not appear to specifically collect biometric information on travelers. It receives information from several US Customs and Border Protection systems and from the FBI’s Terrorist Screening Database. It also collects information about travelers known as a Passenger Name Record from commercial carriers.⁷⁰

Several organizations and individuals submitted comments to the proposed rule.⁷¹ Generally, these comments claim that ATS violates the Privacy Act of 1974, are concerned with the forty-year ATS retention period of information, and are concerned about an individual’s lack of access to ATS records established concerning him or her. The Federal Register notice states that “[g]enerally, this system of records may not be accessed for purposes of determining if the system contains a record pertaining to a particular individual” and “may not be accessed under the Privacy Act for the purpose of inspection.”⁷² The Federal Register notice states that ATS records are exempt from Privacy Act access requirements. In its Privacy Impact Assessment for ATS, DHS states “[t]here is no procedure to correct the risk management and associated rules stored in ATS as the assessment is based on the underlying data and will change when the data from the source system(s) is amended.”⁷³ These statements in the Federal Register and the Privacy Impact Assessment indicate that an individual may not view his own record to determine whether it is accurate. However, the DHS and Department of State program discussed below may help an individual rectify any erroneous information in his or her record, but it appears the individual may not view his or her own record directly.

8. Traveler Redress Inquiry Program (TRIP)

The TRIP was instituted in January 2007 by the DHS and the Department of State to provide travelers with the opportunity to redress problems they had while traveling, such as a delay in or denial of boarding due to DHS screening problems or delayed or denied entry into the United

⁶⁹ *Id.*

⁷⁰ Privacy Impact Assessment for the Automated Targeting System dated August 3, 2007, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atupdate.pdf.

⁷¹ Comments from 30 Organizations and 16 Experts in Privacy and Technology, available at: http://epic.org/privacy/pdf/ats_comments.pdf. Comments from the ACLU, available at: <http://www.aclu.org/privacy/gen/27593leg20061201.html>. Comments from the Electronic Frontier Foundation, available at: http://www.eff.org/files/filenode/travelscreening/ats_comments.pdf. Comments and supplemental comments from The Identity Project and John Gilmore, available at: <http://www.hasbrouck.org/IDP/IDP-ATS-comments.pdf> and <http://www.hasbrouck.org/IDP/IDP-ATS-comments2.pdf>.

⁷² <http://edocket.access.gpo.gov/2006/06-9026.htm>.

⁷³ Privacy Impact Assessment for the Automated Targeting System dated August 3, 2007, pg. 24, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_atupdate.pdf.

States. As part of TRIP, individuals will be required to submit certain identifying and contact information.⁷⁴ TRIP is voluntary so individuals will only have to submit this information upon filing a complaint.⁷⁵ An individual begins the process by filing a complaint either online or by mail.

It appears that TRIP does not permit individuals to access their records directly, but instead implements a grievance process for those who believe their records may be inaccurate due to travel-related problems and delays at security checkpoints.

9. Revisions to the Federal Rules of Civil Procedure

Effective December 1, 2007, the Federal Rules of Civil Procedure underwent major revisions and had a new rule added.⁷⁶ New Rule 5.2 is entitled “Privacy Protection for Filings Made with the Court” and permits documents filed with the court to redact information such as complete social security numbers, birth dates, minors’ full names, and complete financial account numbers.⁷⁷ This Rule was added in compliance with Section 205(c)(3) of the E-Government Act of 2002 (the “E-Government Act”). The E-Government Act requires the US Supreme Court to enact rules “to protect privacy and security concerns relating to electronic filing of documents” and takes notice of the fact that more and more court pleadings are easily available online.⁷⁸

The revision to the Federal Rules is significant because it happens infrequently and shows heightened awareness to the privacy of an individual’s personal information.

Updates to The Original Report

1. Update on the Issue of Whether Biometric Information Maintained by a Government Agency Would be Subject to the Privacy Act of 1974

One of the issues addressed in the Report is the definition of the term “record” under the Privacy Act of 1974 (the “Privacy Act”) and whether a biometric template would be considered a record. The Report included an in depth discussion of how courts have interpreted the term “record” to assist in determining whether biometric information would be subject to the Privacy Act.

To review, the Privacy Act, which covers federal government agencies only and not private individuals or industry, or state and local government agencies, defines “record” as:

“...any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial

⁷⁴ Privacy Impact Assessment for the DHS Traveler Redress Inquiry Program dated January 18, 2007, available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_dhstrip.pdf.

⁷⁵ http://www.dhs.gov/xtrvlsec/programs/gc_1169826536380.shtm#2.

⁷⁶ Jess R. Nix, *The Federal Rules of Civil Procedure Get a Facelift*, THE YOUNG LAWYER, February/March 2008, at 1.

⁷⁷ F.R.C.P. 5.2(a), available at <http://judiciary.house.gov/media/pdfs/printers/110th/civil2007.pdf>.

⁷⁸ Jess R. Nix, *The Federal Rules of Civil Procedure Get a Facelift*, THE YOUNG LAWYER, February/March 2008, at 1.

transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph;”

There remains vast disagreement among the courts as to how broadly to interpret the Privacy Act’s definition of “record.” The United States Supreme Court has only minimally addressed this issue. Such differing interpretations are critical to how broadly a biometric template will be construed as a record. In the only Supreme Court case addressing the issue, which was the 1994 case *U.S. Dept. of Defense v. Federal Labor Relations Authority*,⁷⁹ the Supreme Court applied a broad view of the term “record” in holding that home addresses qualified for protection under the Privacy Act. The Supreme Court ultimately held that the disclosure of the home addresses was a “clearly unwarranted invasion of the employees’ personal privacy within the meaning of the Freedom of Information Act.”⁸⁰ However, the Court did not provide an analysis of the term “records,” but rather, assumed that the home addresses were records.

Accordingly, an examination of the holdings of the lower courts is critical. The Report demonstrated how the Second and Third Circuits have both applied a broad interpretation of the term “records.” Conversely, the Ninth and Eleventh Circuits have adopted very narrow constructions of the term “records,” thereby limiting Privacy Act coverage of personal information maintained by the government.

Since the Report was published, the Fifth Circuit issued a decision where interpretation of the term “record” was a key issue. In *Jacobs v. National Drug Intelligence Center*, the Fifth Circuit Court of Appeals adopted a broad interpretation of the term “record” by looking at the legislative history, which the court believes supports a broader interpretation than the one advanced by the National Drug Intelligence Center. At issue was whether information about Jacobs that was contained in an executive summary of an internal report leaked by the National Drug Intelligence Center was a record. The court held that the executive summary was a record constituting a violation of the Privacy Act.⁸¹

According to the OMB’s guidelines, even publicly available information, such as newspaper clippings or press releases, can constitute a “record.”⁸² Several courts, including the Eleventh Circuit Court of Appeals, have agreed with this interpretation.⁸³ Under such an interpretation, a biometric would constitute a record subject to the Privacy Act even if it was construed as publicly available information, since biometrics are certainly no more public than published information,

⁷⁹ 510 U.S. 487 (1994).

⁸⁰ *Id.* at 489.

⁸¹ *Jacobs v. National Drug Intelligence Center*, 423 F.3d 512 (5th Cir. 2005)

⁸² See OMB Guidelines, 40 Fed. Reg. 56,741, 56,742 (1975) (“[c]ollections of newspaper clippings or other published matter about an individual maintained other than in a conventional reference library would normally be a system of records”).

⁸³ See *Clarkson v. IRS*, 678 F.2d 1368, 1372 (11th Cir. 1982) (permitting challenge to agency’s maintenance of newsletters and press releases); *Murphy v. NSA*, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,389, at 82,036-37 (D.D.C. Sept. 29, 1981) (permitting challenge to agency’s maintenance of newspaper clippings).

It should be noted that many biometric “records” are often one-way encrypted digitized representations that reveal nothing about the person. As such, they may be less likely to be deemed “records” under the Privacy Act. In iris identification, for example, there is no need to have any personal information maintained in the database. All that is needed is the encrypted template for the access control system to function. Thus, to fall under the Privacy Act, such encrypted template (separate from the biometric) would itself have to be deemed a record. Because the encrypted template cannot be traced to the person from whom it was taken, it is highly questionable whether an encrypted template is a record if there is no other personally identifying information or other personal information attached to it.

2. Update on the Privacy Cases Against the Airlines

The Report noted that biometric information of airline passengers is subject to the same rules and afforded the same protections as all other passenger information. Accordingly, if an airline commits to not disclosing passenger information, that commitment extends to a passenger’s biometric data. We reported on several cases that were pending against various airlines concerning the release of passenger data. The following is a status update of those cases.

In a case against Jetblue, consumers filed nine separate class action suits for privacy violations in connection with Jetblue’s release of their passenger information, which they claimed was in violation of state and federal privacy rights. The plaintiffs alleged violations under The Electronic Communications Privacy Act of 1986 and under various state statutory laws regarding unfair and deceptive acts and practices, consumer fraud, and deceptive business practices. They also alleged common law claims for breach of contract, trespass to property, and unjust enrichment. These cases were subsequently consolidated into one case, *In re: Jetblue Airways Corp. Privacy Litigation*, and transferred to the United States District Court for the Eastern District of New York on Feb 24, 2004. The consolidated case was dismissed. The court found that although the airline had violated its own privacy agreement, the plaintiffs failed to prove that they had been harmed by the breach. Accordingly, unless there are significant statutory damages or penalties, a violation of one’s privacy may be an unsustainable claim without proof of actual damages. The plaintiff did not seek injunctive relief.⁸⁴

A similar case against Northwest Airlines filed a couple of months after the JetBlue claim was also dismissed. On January 20, 2004, EPIC and Minnesota Civil Liberties Union (MCLU) filed a complaint against Northwest Airlines saying they engaged in unfair and deceptive practice in violation of the FTC Act⁸⁵ in giving out passenger information as part of a government study in 2001.⁸⁶ In Northwest’s Answer to the Complaint, Northwest stated as its defense that “the privacy rights advocated by EPIC and MCLU do not exist in the rules, precedent or practices of the Department [of Transportation],” that there is “no applicable right to privacy imposed by any

⁸⁴ *In re: JetBlue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299 (E. D. N.Y. 2005).

⁸⁵ Note that the FTC Act does not mention privacy. The statute is limited to prohibiting “unfair methods of competition” and “unfair or deceptive acts” in commerce.

⁸⁶ *In the Matter of Northwest Airlines, Inc.*, Docket OST-04-16939-1, Complaint and Request for investigation, injunction, and for other relief, 1 (January 20, 2004), at http://www.epic.org/privacy/airtravel/nwa_comp.pdf, also available at Department of Transportation, Docket Management System, <http://dms.dot.gov/>. This complaint action is currently pending. See Department of Transportation, Docket Management System, Docket OST-04-16939, <http://dms.dot.gov>

other federal law,” that “passengers have no inherent right or expectation of total privacy in the information they provide when traveling on commercial airlines,” and that “the only basis for any right to privacy on the part of customers of Northwest” is Northwest’s privacy policy.⁸⁷ On June 6, 2004, the United States District Court, District of Minnesota dismissed the case.⁸⁸ The court found no direct harm and held that the release of passenger information under the circumstances was not an unreasonable disclosure, stating:

In this instance, Plaintiffs voluntarily provided their personal information to Northwest. Moreover, although Northwest had a privacy policy for information included on the website, Plaintiffs do not contend that they actually read the privacy policy prior to providing Northwest with their personal information. Thus, Plaintiffs’ expectation of privacy was low. Further, the disclosure here was not to the public at large, but rather was to a government agency in the wake of a terrorist attack that called into question the security of the nation’s transportation system. Northwest’s motives in disclosing the information cannot be questioned. Taking into account all of the factors listed above, the Court finds as a matter of law that the disclosure of Plaintiffs’ personal information would not be highly offensive to a reasonable person and that Plaintiffs have failed to state a claim for intrusion upon seclusion.⁸⁹

In June 2002, it was reported by the Associated Press that American Airlines acknowledged it had shared approximately 1.2 million passenger itineraries with the Transportation Security Administration.⁹⁰ No lawsuits have been filed against American Airlines. Perhaps this is because at the time the itineraries were shared, American Airlines did not have a privacy policy expressly prohibiting the sharing of passenger data providing no basis for a passenger’s expectation of privacy.

It is interesting to note that the Privacy Act of 1974 governs the collection of information by a federal government agency. It is unclear why the passengers did not bring an action against the government for improper collection of personal information.

3. Update on the US-VISIT Program – International Travel

The Report included a discussion of the US-VISIT program which is one of the most important programs relating to the use of biometrics. The program is the culmination and implementation of a number of different legislative acts intending to ensure the accurate tracking of foreign nationals entering and exiting the United States.⁹¹

⁸⁷ *Id.* at 3. A copy of the Answer of Northwest Airlines, Inc., can be found on EPIC’s website at http://www.epic.org/privacy/airtravel/nwa_answer.pdf.

⁸⁸ *In re Northwest Airlines Privacy Litigation*, 2004 U. S. Dist. LEXIS 10580 (June 6, 2004).

⁸⁹ *Id.* at 5.

⁹⁰ Brad Foss, *Airline Admits Giving U.S. Passenger Data*, THE ASSOCIATED PRESS, April 9, 2004.

⁹¹ For a complete recitation of the background and the planned implementation of US-VISIT *see* Federal Register / Vol. 69, No. 2, Implementation of the United States Visitor and Immigrant Status Indicator Technology Program (“US-VISIT”); Biometric Requirements; Notice to Nonimmigrant Aliens Subject To Be Enrolled in the United States Visitor and Immigrant Status Indicator Technology System; Interim Final Rule and Notice.

The program was originally limited to holders of certain nonimmigrant visas and was soon expanded to include many non-visa countries, including Canada and the United Kingdom. US-VISIT has since been further expanded to cover virtually all visitors holding non-immigrant visas, regardless of country of origin (with limited exemptions, such as for certain visa holders, most Canadians, some Mexicans, and people under the age of 14 or over the age of 79).⁹² This will include millions of permanent residents and green card holders, who will be required to be fingerprinted and photographed upon re-entering the United States by air or sea. Foreign nationals covered under the program who refuse to provide the requested biometric information upon entry may be deemed inadmissible to the United States for failure to provide the required documentation.

The NBSP US Privacy Report noted that the 9/11 Commission recommended that the US-VISIT program be expanded to include exit data as well as entry data, and, more importantly, that Americans not be exempt from the program. The Department of Homeland Security began testing exit procedures at several airports around the country,⁹³ but, as of May 6, 2007, ended this practice⁹⁴. On May 21, 2008, the US-VISIT Program issued a “Request for Information/Sources Sought” to conduct market research. The US Government issued this Request to identify potential solutions, service providers, and suppliers interested in participating in the design and development of a biometric land exit solution.⁹⁵

Under a nationwide data-sharing program known as the IDENT/IAFIS program, two existing databases are now being used in conjunction with one another as part of the US-VISIT program to prevent illegal entry into the United States. One of those databases is the Automated Biometric Identification System (known as “IDENT”), which is a database system run by the Department of Homeland Security that uses automated fingerprint identification systems technology.⁹⁶ The other database is the Integrated Automated Fingerprint Identification System (IAFIS), which is a national fingerprint and criminal history database operated by the FBI and is the largest biometric database in the world.⁹⁷ Through this new data sharing system, border patrol agents are now able to simultaneously search the IDENT and IAFIS systems to determine whether the individual seeking entry into the United States has an outstanding criminal warrant.⁹⁸ The IDENT/IAFIS program, which began as a pilot program in the San Diego Border Patrol Sectors Brown Field Station and the Calexico Port of Entry in August 2001, is currently operating in every US Customs and Border Protection Border Patrol station throughout the country.⁹⁹ Biometric information contained in the IDENT/IAFIS systems will be available to

⁹² http://www.dhs.gov/xtrvlsec/programs/content_multi_image_0006.shtm.

⁹³ http://www.dhs.gov/xtrvlsec/programs/editorial_0525.shtm.

⁹⁴ *Id.*

⁹⁵

<https://www.fbo.gov/index?tab=core&s=opportunity&mode=form&id=833c071bbc5913a9d93742f903ab7da0&cck=1&au=&cck=>

⁹⁶ www.espionageinfo.com.

⁹⁷ www.fbi.gov.

⁹⁸ www.usinfo.state.gov. See also Department of Homeland Security Press Release dated September 21, 2004 (Department of Homeland Security Announces Biometric Identification System Operational at Border Patrol Stations Nationwide).

⁹⁹ Department of Homeland Security Press Release dated September 21, 2004 (Department of Homeland Security Announces Biometric Identification System Operational at Border Patrol Stations Nationwide).

other organizations, including federal, state, and foreign agencies.¹⁰⁰ On September 1, 2006, the Department of Homeland Security's US-VISIT Program Office issued a Privacy Impact Assessment (PIA) for the Interim Data Sharing Model for the IDENT and IAFIS Interoperability Project. The PIA discusses the sharing of data between IDENT and IAFIS and the Department of Homeland Security's sharing of IDENT data with the FBI. (An earlier PIA issued by the FBI addressed the IAFIS data that the FBI shares with the Department of Homeland Security.) According to the PIA, the FBI runs a query using the biometric and biographical data against the stored IDENT data. The query results are returned to the FBI and any positive matches are forwarded to the Law Enforcement Support Center of Immigrations and Customs Enforcement for data verification and interpretation. The FBI must receive data verification and interpretation of the IDENT data back from the Law Enforcement Support Center of Immigrations and Customs Enforcement prior to taking any action based on such data.

Because the US-VISIT program uses widely accessible systems to verify identity and compares the data against law enforcement data and watch lists, and because the data collected will be maintained in the United States, the program raises many issues and concerns regarding data privacy, particularly for those countries whose citizens are required to submit personal data. Many of those countries (including the European Union) have far more stringent regulations governing privacy and the collection, use, and safeguarding of personal data than does the United States. One of the difficulties in implementing the US-VISIT program has been acceptance by other countries. In August 2007, the European Union and the US entered into an agreement regarding transferring Passenger Name Record data to DHS. Although this does not specifically apply to the US-VISIT program, the European Union has made concessions regarding US privacy policy.

4. Update on The Real ID Act

The Real ID Act was signed into law on May 11, 2005 after passing through the Senate with a 100-0 vote.¹⁰¹ The Real ID Act imposes certain federal requirements on state-issued driver's licenses and identification cards. Immigration and civil liberties groups believe it is a prelude to a national identification card and are calling it an attack not only on privacy, but also on refugees and asylum-seekers. Supporters, on the other hand, believe the Real ID Act will make US borders safer.¹⁰²

The REAL ID Act requires states to verify certain personal identification documents before issuing a driver's license. The REAL ID Act also requires all driver's licenses and identification cards to contain certain uniform information, including, at minimum, the individual's full legal name, signature, date of birth, gender, identification number, and principal residence address. Driver's licenses and identification cards must also contain a photograph of the individual, security features designed to prevent counterfeiting or tampering, and a common machine-readable technology with defined minimum data elements. These data elements are not set out in

¹⁰⁰ Adam Chandler. DHS Expands its Biometric Database. July 27, 2006, at www.fcw.com/article95440-07-27-06-Web.

¹⁰¹ With respect to the bill's unanimous passage in the Senate, it should be noted that critics of the legislation point to the fact that it was attached to "must-pass" legislation for funding military action in Iraq.

¹⁰² <http://washingtontimes.com/upi-breaking/20050509-050110-3715r.htm>.

the REAL ID Act, but are left to the determination of the Secretary of Homeland Security, the Secretary of Transportation, and the states.¹⁰³ State officials participated with DHS in the development of the final rule.¹⁰⁴

Additionally, the Act requires proof that the person seeking the identification card is lawfully present in the United States. The Washington Post reported that seven of the 9/11 hijackers received driver's licenses or other identification cards in Virginia. Prior to 2001, Virginia did not require proof of legal presence in the United States before issuing a driver's license.¹⁰⁵ Presumably, had the Real ID Act been in place prior to 9/11, those hijackers who were not lawfully in the United States would not have been able to obtain driver's licenses or other identification cards from any state in the United States.

Supporters of the Real ID Act claim that all the new federal law does is require states to vouch for the authenticity of the person presenting a driver's license: in other words, making sure that the person seeking a driver's license is who they claim to be, making it more difficult to obtain, make, or use fake IDs.

However, there are many opponents of the new law, including the ACLU, Privacy International, the National Governors Association, the National Conference of State Legislatures, the American Association of Motor Vehicle Administrators, and Council of State.¹⁰⁶ Among the expressed concerns are that the Act actually increases the risk of identity theft by linking electronically machine-readable digital photographs and addresses on state Department of Motor Vehicle computers nationwide. "The federalization of drivers' license and the culling of all information into massive databases creates a system ripe for identity theft," the ACLU said.

The fundamental purpose and operation of the Act has changed little since it passed, and state governments and departments of motor vehicles remain concerned over the logistics of implementing it. States have expressed concerns that the costs of implementation are significantly higher than Congress estimated and that they will not be able to meet the implementation deadline.¹⁰⁷

In September 2006, a report titled "The Real ID Act: National Impact Analysis" was issued by a coalition of state governors, state legislative groups, and representatives from the American Association of Motor Vehicle Administrators (the "Real ID Report"). The Real ID Report concludes that states have been given no real implementation guidelines and it projects that the cost of implementation will be around \$11 billion, which is more than 100 times the \$100 million Congress estimated when it passed the bill. The report breaks down the total cost by analyzing and estimating the cost of implementation of each of the Act's requirements. The report recommends that Congress extend the deadline to give states more time to not only implement the new identification cards, but also to assess security safeguards.¹⁰⁸

¹⁰³ <http://www.ncsl.org/print/standcomm/sctran/realidsummary05.pdf>.

¹⁰⁴ http://www.dhs.gov/xprevprot/laws/gc_1172767635686.shtm.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

¹⁰⁷ Yegyazarian, Anush. Tech.gov: Real ID's Real Problems. PC World. October 11, 2006.

¹⁰⁸ A separate report issued by INPUT [INPUT is a company providing market information to help private companies procure government contracts and is the self-proclaimed "authority on government business."] estimates

The Real ID Report also noted that, with respect to the facial image capture requirement, that the report's projected cost of \$248 million for this aspect of the implementation process does not include the facial imaging recognition software needed to compare captured images with existing images in state databases. The report states that "[a]lthough photo capture of all applicants is a useful tool; its effectiveness is diminished greatly without a significant investment in facial recognition technology."¹⁰⁹

The California state legislature has already issued a set of security safeguard principles in response to the Real ID Act. Included in these principles are protections aimed specifically at the use of radio frequency identification (RFID) technology, since that is one of the technologies in strong contention for use in both the state identification cards and e-passports.¹¹⁰ Although Governor Schwarzenegger vetoed the bill in September 2006, the bill could serve as a model for other states or a national standard.¹¹¹

States are free to issue non-complying licenses and identification cards, but they may not be accepted for any federal identification purposes, including travel on common carrier aircraft or entering federal buildings and facilities, unless the individual undergoes additional screening.¹¹²

The REAL ID Act is experiencing serious opposition from the states. On January 25, 2007, the Maine Legislature overwhelmingly voted to pass "An Act to Prohibit Maine from Participating in the Federal REAL ID Act of 2005". The bill was subsequently enacted as 29-A M.R.S. § 1411 and summarily proscribes the Maine Secretary of State from amending the driver license law to conform to the Act.¹¹³

Montana followed suit in April 2007 by enacting Mont. Code Anno., § 61-5-128 which not only declares that Montana will not participate in the implementation of the REAL ID Act, but also requires the Motor Vehicle Division "to report to the governor any attempts by the Department of Homeland Security to secure the implementation of the act."¹¹⁴

Additional states that have passed legislation opposing the REAL ID Act, either by prohibiting compliance or by urging the President and Congress to repeal it, include Arizona, Idaho, Washington, North Dakota, Nevada, Hawaii, Colorado, Nebraska, Oklahoma, Missouri, Arkansas, Illinois, Tennessee, Georgia, South Carolina, and New Hampshire. Bills opposing the REAL ID Act have passed one chamber of the state legislature in South Dakota, Michigan, Oregon, Wyoming, Utah, New Mexico, Minnesota, Louisiana, West Virginia, Pennsylvania, and Vermont. Finally, bills opposing the REAL ID Act have been introduced in Alabama, Alaska,

the cost at only \$2.5 billion, which is still significantly higher than Congress's original estimate. See INPUT Press Release August 30, 2006.

¹⁰⁹ The Real ID Act: National Impact Analysis. September 2006. Page 11.

¹¹⁰ RFID can be used to track the movement of the cards, and thus the person carrying the card. See Anita Ramasastry, Why the 'Real ID' Act is a real mess. CNN.com. August 12, 2005.

¹¹¹ Yegyazarian, Anush. Tech.gov: Real ID's Real Problems. PC World. October 11, 2006.

¹¹² http://www.dhs.gov/xprevprot/programs/gc_1172767635686.shtm.

¹¹³ <http://www.mainelegislature.org/legis/bills/billpdfs/LD113802.pdf>.

¹¹⁴ <http://public.cq.com/docs/hs/hsnews110-000002491548.html>.

California, Washington, D.C., Texas, Wisconsin, Ohio, Kentucky, Mississippi, Maryland, New York, North Carolina, Rhode Island, Virginia, and Massachusetts.¹¹⁵

After several prior extensions, states were supposed to be in full compliance with the REAL ID Act by May 11, 2008. However, this deadline can be delayed until May 11, 2011 by timely filing requests for extensions. In the Final Rule on the Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, published in the Federal Register on January 29, 2008 and effective March 31, 2008, the Department of Homeland Security offered extensions in compliance to states as long as they apply by March 31, 2008. These extensions will terminate on December 31, 2009, unless the states apply for an additional extension by October 11, 2009. These additional extensions will terminate May 11, 2011. After that, federal facilities and agencies will no longer accept state driver's licenses or identification cards that do not comply with the REAL ID Act.

Despite the number of states passing legislation to oppose the REAL ID Act, 47 of the 50 states have sought extensions or taken other steps to move toward compliance with the REAL ID Act while only three (South Carolina, Maine, and Montana) have refused to take any action conforming with the REAL ID Act.¹¹⁶ Lawmakers in South Carolina petitioned their governor to request the extension for compliance offered by the federal government so that South Carolina citizens would not be forced to comply with the REAL ID Act.¹¹⁷ The governor requested the extension shortly before the deadline¹¹⁸. If he had not done so, individuals holding a driver license issued by the state of South Carolina will encounter problems and delays when using their driver licenses to board domestic flights.¹¹⁹

It appears that the states' major concerns include apprehension over implementation costs for the states and whether the REAL ID Act actually creates a national identification card as opposed to concerns about the information contained on the card.

5. Update on CAPPS (Computer Assisted Passenger Pre-Screening System) II and the Secure Flight Program – Domestic Flights

The Report included a discussion of CAPPS II (the passenger screening system for domestic flights that was the successor to the original CAPPS system that was in place on September 11, 2001). The Report noted that there were many privacy concerns about the CAPPS II system and that there were rumors of a merger between CAPPS II and the US-VISIT program that were raising additional concerns. These concerns were causing delays in implementing the CAPPS II system.

On August 26, 2004, shortly after the Report was published, the Transportation Security Administration ("TSA") announced that it was replacing CAPPS II with a new program called Secure Flight. Under Secure Flight, passenger name records are matched against a list of

¹¹⁵ <http://www.realnightmare.org/news/105/>.

¹¹⁶ <http://www.cnn.com/2008/US/03/21/Real.Ids.ap/index.html?iref=newssearch>.

¹¹⁷ *Id.*

¹¹⁸ <http://blog.wired.com/27bstroke6/2008/03/defiant-south-c.html>

¹¹⁹ *Id.*

suspected terrorists using watch lists held in the Terrorist Screening Database.¹²⁰ Secure Flight is limited to domestic flights. International terrorist screening will continue to be conducted by US Customs and Border Protection.¹²¹

The key difference between CAPPs II and Secure Flight is that Secure Flight only looks for known or suspected terrorists, and does not seek to find other law enforcement violators. However, privacy advocacy groups continue to express concerns about the new screening system particularly with respect to the integrity of the watch lists, pointing to certain high-profile incidents (such as when Senator Edward Kennedy and Cat Stevens were each stopped before boarding a flight because their names matched individuals on terrorism watch lists had used those names as aliases) as illustrations of the current system's failings.¹²²

The Transportation Security Administration held a public meeting regarding the Notice of Proposed Rulemaking on September 20, 2007.¹²³ Although the program has not yet been implemented, the Transportation Security Administration website declares it is taking "significant steps" toward execution of this program.¹²⁴

There have been approximately 100 comments to this proposed rule as of September 2007. Comments indicate individuals' fears that the Secure Flight program will interfere with Americans' right to travel as well as concerns from the Association of Corporate Travel Executives that the Secure Flight Program does not provide redress for passengers on the "No Fly" list or give sufficient information on who has access to the data collected and how it is stored.¹²⁵ The Traveler Redress Inquiry Program (TRIP) may be useful to a traveler who encounters problems. The comment period ended October 22, 2007.¹²⁶

In a statement given to the Subcommittee on Homeland Security and Committee on Appropriations in the House of Representatives, Kip Hawley, Assistant Secretary of TSA, stated it was TSA's goal was to have the Secure Flight program begin testing by the end of 2008 and operational in 2010.^{127 128}

¹²⁰ Larry Greenemeier, Transportation Security Administration Set to Collect Passenger Data From Airlines, INFORMATION WEEK, September 27, 2004, at <http://www.informationweek.com/shared/printableArticle.jhtml?articleID=47902823>

¹²¹ *Id.*

¹²² *Id.*

¹²³ http://www.tsa.gov/what_we_do/layers/secureflight/index.shtm.

¹²⁴ *Id.*

¹²⁵ <http://dms.dot.gov/search/searchResultsSimple.cfm>.

¹²⁶ http://www.tsa.gov/assets/pdf/secureflight_meeting.pdf.

¹²⁷ http://www.tsa.gov/assets/pdf/hahsc_security_challenges.pdf.

¹²⁸ http://www.tsa.gov/press/journal/secure_flight.shtm.