IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

Case No. CJ-2011-1469

STATE OF OKLAHOMA } S.S.
CLEVELAND COUNTY }
FILED

JUN 19 2013

In The Office of the
Court Clerk RHONDA HALL

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

COMES NOW the Plaintiff, Kaye Beach ("Ms. Beach"), by and through her attorneys of record M. Eileen Echols and Benjamin P. Sisney, of Echols, Echols & Smalley, and Douglas R. McKusick, of the Rutherford Institute, pursuant to 12 O.S. §2056 and Rule 13, Rules For District Courts, 12 O.S. Supp. 2010, 12 O.S. ch. 2, app., and moves this Court to enter Summary Judgment as to Count I against the Defendants, Oklahoma Department of Public Safety, Defendant Michael C. Thompson, Commissioner of the Oklahoma Department of Public Safety, in his official and individual capacity, and Ricky G. Adams, Assistant Commissioner of the Oklahoma Department of Public Safety, in his official and individual capacity, (the "State"). In support of her Motion for Summary Judgment, Ms. Beach alleges and states as follows:

I. LEGAL STANDARDS OF SUMMARY JUDGMENT

"The judgment sought should be rendered if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." 12 O.S. §2056(C). Summary judgment is properly granted "when the pleadings, affidavits, depositions, admissions or other evidentiary materials establish that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Davis v. Leitner*, 1989 OK 146, ¶ 9, 782 P.2d 924, 926. Although a trial court considers factual matters when deciding whether summary judgment is appropriate, its ultimate decision is purely legal: "whether one party is entitled to judgment as a matter of law because there are no material disputed factual questions." *Carmichael v. Beller*, 1996 OK 48, ¶ 2, 914 P.2d 1051, 1053.

II. STATEMENT OF UNDISPUTED MATERIAL FACTS.

1. Ms. Beach is a resident of the State of Oklahoma and of Cleveland County, Oklahoma. *See* Exhibit 1, Affidavit of Kaye Beach, ¶1.[1]

2. Defendant Oklahoma Department of Public Safety constitutes a "Governmental entity" as defined by the Oklahoma Religious Freedom Act. Okla. Stat. tit. 51, § 252(5). Admitted by Defendants at ¶2 of Defendant's Answer, attached as Exhibit 2.

3. On March 8, 2011, Ms. Beach attempted to apply for a renewal driver's license at Fusion Tag Agency (the "Tag Agency") located at1236 North Interstate Drive, Norman, OK 73072, in Cleveland County, Oklahoma. *See* Exhibit 1, Affidavit of Kaye Beach, ¶2.

---

[1]The entirety of Ms. Beach's Affidavit attached hereto as Exhibit 1 is incorporated by reference as if fully set forth herein.

4. The Fusion Tag Agency is a motor license agent/agency of the Oklahoma Tax Commission and has been approved by Defendant Oklahoma Department of Public Safety ("DPS") to issue driver license and identification (DL/ID) cards, as contemplated in 47 O.S. §§ 1140 et seq. Admitted by Defendants at Response for Request for Admission No. 10, attached as Exhibit 3.

5. Notwithstanding her satisfaction or ability to satisfy any other relevant requirements for obtaining a renewal driver's license, Ms. Beach's attempt to apply was rejected by the Tag Agency. *See* Exhibit 1, Affidavit of Kaye Beach, ¶3.

6. The Tag Agent informed Ms. Beach it was required by law to take a high-resolution digital facial photograph, and that she could not apply for or obtain a renewal license without allowing the DPS agent to capture her biometric facial photograph or fingerprints. *See* Exhibit 1, Affidavit of Kaye Beach, ¶4.

7. Ms. Beach requested and was denied an accommodation on account of her sincerely held religious beliefs and religiously motivated practice, which are more fully set forth below. *See* Exhibit 1, Affidavit of Kaye Beach, ¶5.

8. Later that same day, March 8, 2011, Ms. Beach contacted DPS directly and again explained her religious objection and requested an accommodation. On or about March 11, 2011, Ms. Beach followed up by telephone and was informed by a DPS employee, Mr. Steve Grunyard, that the biometrics were required by law and that there would be no accommodation or alternative. *See* Exhibit 1, Affidavit of Kaye Beach, ¶6.

9. On March 18, 2011, Ms. Beach sent a letter to DPS identifying her religious objections and requesting an accommodation. Ms. Beach informed DPS that she does not object to a low-resolution facial photograph. Ms. Beach also specifically asked, "Are there

any available administrative remedies that I can pursue that I have not pursued to this point or have I exhausted all administrative remedies." *See* Exhibit 1, Affidavit of Kaye Beach, ¶7; *see also* Exhibit 4, Ms. Beach's Letter to DPS dated March 18, 2011.

10. On April 27, 2011, she received an email from Stephen J. Krise, General Counsel, Oklahoma Department of Public Safety, stating as follows:

> I'm sorry I missed your call, but I have obtained information related to your question of whether there is an alternative to having a driver license photograph that does not capture facial recognition features, commonly referred to as biometric data. Such photographs are required by statute and the law does not provide for an alternative or exemption.

See Exhibit 1, Affidavit of Kaye Beach, ¶8; Exhibit 5, Email Correspondence from Mr. Krise dated April 27, 2011.

11. On June 5, 2011, Ms. Beach received a criminal citation for a violation described as "EXPIRED DRIVER'S LICENSE, with a notation identifying Norman Municipal Code Section 20-509(a), entitled "Driving: License of driver." This municipal ordinance, in pertinent part, provides that "[n]o person shall operate any vehicle upon the streets of the City without that person being licensed in the manner now required by the laws of the State of Oklahoma, which are hereby incorporated into the Code of the City of Norman as if fully set out in this subsection." Norman Municipal Code, Sec. 20-509(a). *See* Exhibit 1, Affidavit of Kaye Beach, ¶9; *see* Exhibit 6, copy of Citation.

13. On July 18, 2011, Ms. Beach again attempted to obtain a renewal driver's license at Fusion Tag Agency in Norman, Oklahoma, and was again denied on account of her religiously motivated inability to allow the Tag Agent to capture her biometrics. *See* Exhibit 1, Affidavit of Kaye Beach, ¶10.

14. On July 21, 2011, Ms. Beach appeared with her counsel at the Norman Municipal Courthouse for her arraignment, where a Norman Assistant City Attorney dismissed the charge. *See* Exhibit 1, Affidavit of Kaye Beach, ¶11.

15. As a result of the State's refusal to provide an accommodation, Ms. Beach is unable to lawfully drive a motor vehicle and in fact was criminally charged for driving without a valid driver's license; Ms. Beach has been denied the ability to acquire prescription medication; Ms. Beach has been denied the ability to use her debit card; Ms. Beach has been denied the ability to rent a hotel room; and Ms. Beach has been denied the ability to obtain a P.O. box. *See* Exhibit 1, Affidavit of Kaye Beach, ¶12.

16. Ms. Beach is forbidden by her sincerely held religious beliefs to allow a high-resolution facial photograph, or facial biometric, or other biometrics, in a format compliant with international standards, to be captured by DPS. *See* Exhibit 1, Affidavit of Kaye Beach, ¶13.

17. Ms. Beach has learned and believes that the interoperability and open architecture format for the high-resolution biometric facial photograph used by motor license agents as required by DPS to take the photographs for driver's licenses is an internationally set format determined by the United Nations' International Civil Aviation Organization ("ICAO") intended to be "interoperable," and that the database into which her biometric data is placed is managed and accessed by a self-described international organization called the American Association of Motor Vehicle Administrators ("AAMVA") and/or its member jurisdictions and corporate entities. *See* Exhibit 1, Affidavit of Kaye Beach, ¶14 (a more detailed statement and supporting documentation is provided in Ms. Beach's Affidavit); see State's Answer to Interrogatory No. 12, attached as Exhibit 7 ("DPS follows the American

Association of Motor Vehicle Administrator standards.").

18. In its Answer to Interrogatory No. 13, which asked: "Please identify the role, function and input, if any, of the Department of Public Safety in the establishment of the standard for the resolution and format of the biometric information collected from Drivers License and Identification Card Applicants," the State responded: "DPS follows the American Association of Motor Vehicle Administrator standards." State's Answer to Interrogatory No. 13, attached as Exhibit 7.

19. The State identified "MorphoTrust USA" as an entity that has access to the database in which Drivers License and Identification Card Applicants' biometric data is stored, *see* State's Answer to Interrogatory No. 3, attached as Exhibit 8, and that "MorphoTrust USA" provides the management, maintenance, hardware, software, logistical support, or any other type of support regarding the databases in which said biometric information is stored, *see* State's Answer to Interrogatory No. 4, attached as Exhibit 8.

20. The State identified "[t]he L-1 Contract" as the contract between the State and another entity regarding the collection, storage, use, sharing or access of the biometric information of Driver License and Identification Card Applicants. *See* State's Answer to Interrogatory No. 21, attached as Exhibit 9.

21. "MorphoTrust USA, Inc. was formed when L-1 Identity Solutions was acquired in July 2011 by Safran, a global technology powerhouse in aerospace, defense, and security and an international top-tier supplier of systems and equipment. MorphoTrust is a Morpho company and part of Safran Group." MorphoTrust USA website, "Our History," at http://www.morphotrust.com/pages/204-history, attached as Exhibit 10.

22. MorphoTrust/L-1/Safran Group provides driver license and digital identification services to Latvia, Costa Rica, Mexico, and Ghana, to name a few. *Id.* Safran is based in France. According to its website, "Safran is a global group, with operations on five continents," including significant operations in China and Russia. Safran website, "Our Sites," at http://www.safran-group.com/site-safran-en/group/safran-worldwide/our-sites/?345, attached as Exhibit 11.

23. "Recognizing the development of standards is crucial to the mass adoption of biometrics, L-1 Identity Solutions actively participates in both nationally-and internationally-recognized standards initiatives." L-1 website, as of August 20, 2012, "Standards," attached as Exhibit 12.

24. Ms. Beach's religiously motivated practice is abstaining from allowing her biometric information to be captured, placed into a database and linked with other entities and jurisdictions in an international system of identification she believes manifests certain Biblical prophecies and prohibitions. *See* Exhibit 1, Affidavit of Kaye Beach, ¶15.

25. Ms. Beach's religiously motivated practice is based on her sincerely held religious beliefs that the Bible, specifically Revelations 13: 16-18 and 14:9-11, explicitly commands believers to not participate in a global numbering identification system using the number of man, and eternally condemns participation in that system. *See* Exhibit 1, Affidavit of Kaye Beach, ¶¶16, 17.

26. Ms. Beach's religiously motivated practice is and arises from a sincerely held religious belief. Put simply, "bio" means "body" and "metric" means "measurement." Hence, a biometric is the number of the body of man, which Ms. Beach believes Revelations explicitly forbids her from submitting into the international and interoperable

system described above. *See* Exhibit 1, Affidavit of Kaye Beach, ¶17; and, Exhibit 13, Letter from Pastor Kevin Clarkson of First Baptist Church of Moore.

27. The State refuses to provide an accommodation to Ms. Beach based on her sincerely held religious beliefs and religiously motivated practice to allow her to obtain a driver's license without submitting her biometric information. *See* Exhibit 1, Affidavit of Kaye Beach, ¶18; *see* Exhibit 5, Email Correspondence from Mr. Krise dated April 27, 2011.

28. The State's sole asserted purpose for its refusal to provide a religious accommodation to Ms. Beach is that "[a]llowing exceptions would open the door for unlimited requests for exceptions and defeat the purpose of having such stringent identity verification measures. Religion does not play a role in this process." *See* State's Answer to Interrogatory No. 1, attached as Exhibit 14. Further, "[t]he purpose for collecting biometric images is to verify that the person applying for a DL/ID card is that person." *Id.*

29. In her Request for Production No. 11, Ms. Beach requested the State to "provide complete copies of any document containing the Department of Public Safety's stated purpose(s) or from which the stated purpose(s) are derived in whole or in part, for refusing to provide a religious accommodation for Drivers License and Identification Card Applicants that would allow an Applicant to submit a non-biometric facial photograph and not submit fingerprints. In its Response, the State answered: "No documents to produce." *See* Ms. Beach's Request for Production No. 11 and State's Response, attached as Exhibit 15.

30. The State's sole asserted compelling governmental interest in refusing to provide an accommodation to Ms. Beach on account of her sincerely held religious beliefs and

religiously motivated practice is that "[t]he State of Oklahoma is required by Federal law to gather biometric data as part of its motor vehicle licensing process and there is a compelling governmental interest in complying with the applicable Federal laws." *See* State's Answer, Affirmative Defenses at p. 6, ¶5, attached as Exhibit 16.

31. In fact, there is no federal law requiring the State to gather biometric data as part of its motor licensing process, as the State now admits. *See* State's Answer to Interrogatory No. 6, attached as Exhibit 17.

32. The State admits "there are other ways to confirm identity" than to require DL/ID applicants to submit biometric information. *See* State's Answer to Interrogatory No. 1, attached as Exhibit 14.

33. The State admits "that an individual's birth certificate is considered a primary form of ID. Applicants must also provide a secondary form of ID." *See* State's Response to Request for Admission No. 11, attached as Exhibit 3.

34. Ms. Beach has a birth certificate which has previously been accepted as a primary form of identification by DPS and the tag agent and has secondary forms of ID to satisfy the non-objectionable identification requirements. *See* Exhibit 1, Affidavit of Kaye Beach, ¶19.

35. The State asserts "[t]here are no less restrictive means used by the Department that would verify identity to that level of certainty and with the same degree of security," than requiring DL/ID card applicants to submit biometric information. *See* State's Answer to Interrogatory No. 1, attached as Exhibit 14.

36. Breeder documents, such as birth certificates, establish a person's identity, not

biometrics. Biometrics simply attempt to link a person to the already established identity created by the breeder documents. *See* Mercer, John, "Breeder Documents, The Keys to Identity," *Keesing Journal of Documents & Identity*, p.14, issue 29, 2009, attached as Exhibit18.

III. THE LAW AT ISSUE: THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT.

Following the oft criticized United States Supreme Court opinion in *Employment Div. v. Smith*, 494 U.S. 872, 110 S. Ct. 1595 (1990), which held that neutral laws of general applicability were not subject to strict scrutiny for purposes of the First Amendment,[2] numerous States passed variations of religious freedom acts in an effort to statutorily protect religious free exercise beyond the *Smith* standard by restoring the strict scrutiny standard of *Sherbert v. Verner*, 374 U.S. 398, 83 S. Ct. 1790 (1963), and *Wisconsin v. Yoder*, 406 U.S. 205, 92 S. Ct. 1526 (1972). *See Barr v. City of Sinton*, 295 S.W.3d 287, 296, 52 Tex. Sup. J. 871 (2009) ("*Smith*'s construction of the Free Exercise Clause does not preclude a state from requiring strict scrutiny of infringements on religious freedom, either by statute or under the state constitution, and many states have done just that").[3] In

---

[2]*See Gonzales v. O Centro Espirita Beneficente Uniao do Vegetal*, 546 U.S. 418, 424, 126 S. Ct. 1211 (2006) ("In *Employment Div., Dept. of Human Resources of Ore. v. Smith*, 494 U.S. 872, 110 S.Ct. 1595, 108 L.Ed.2d 876 (1990), this Court held that the Free Exercise Clause of the First Amendment does not prohibit governments from burdening religious practices through generally applicable laws.").

[3]In *Employment Div. v. Smith*, the United States Supreme Court held that neutral laws of general applicability were not subject to "strict scrutiny." *See Smith*, 494 U.S. at 879, 110 S. Ct. at 1600 ("the right of free exercise does not relieve an individual of the obligation to comply with a 'valid and neutral law of general applicability on the ground that the law proscribes (or prescribes) conduct that his religion prescribes (or proscribes)." (internal quotation marks and citation omitted)). The ORFA is meant to restore pre-*Smith* free exercise jurisprudence as applied to neutral and generally applicable laws. It is logical, then, to consider the views of the four Justices that did not join the Court in *Smith*: "Once it has been shown that a government

2000, Oklahoma jointed the States desiring to restore the heightened strict scrutiny standard by enacting the Religious Freedom Restoration Act (ORFA, the "Act"), Okla. Stat. tit. 51, §§ 251 - 258.

Pursuant to the Oklahoma Religious Freedom Restoration Act,

> no governmental entity shall substantially burden a person's free exercise of religion even if the burden results from a rule of general applicability . . . unless it demonstrates that application of the burden to the person is: 1. Essential to further a compelling governmental interest; and 2. The least restrictive means of furthering that compelling governmental interest.

Okla. Stat. tit. 51, § 253. "'Demonstrates' means the burdens of going forward with the evidence and of persuasion under the standard of clear and convincing evidence are met." *Id.* at § 252(1). "'Exercise of religion' means the exercise of religion under Article 1, Section 2, of the Constitution of the State of Oklahoma, the Oklahoma Religious Freedom Act, and the First Amendment to the Constitution of the United States." *Id.* at § 252(2). "'Substantially burden' means to inhibit or curtail religiously motivated practice." *Id.* at § 252(7).

Accordingly, all Ms. Beach must prove is that her religiously motivated practice have been substantially burdened, *i.e.*, inhibited or curtailed, by the State. It is then the State's burden to demonstrate with clear and convincing evidence that its denial of Ms. Beach's religious accommodation is essential to further a compelling governmental interest; *and* the least restrictive means of furthering that compelling governmental interest.

---

regulation or criminal prohibition burdens the free exercise of religion, we have consistently asked the government to demonstrate that the unbending application of its regulation to the religious objector is essential to accomplish an overriding government interest . . . or represents the least restrictive means of achieving some compelling state interest." *Id.* at 899 (internal quotation omitted). The ORFA resurrected that standard and this Court should employ it.

IV. LEGAL ARGUMENT AND APPLICATION.

A. Ms. Beach's Religiously Motivated Practice.

For purposes of the Act, the "'Exercise of religion' means the exercise of religion under Article 1, Section 2, of the Constitution of the State of Oklahoma, the Oklahoma Religious Freedom Act, and the First Amendment to the Constitution of the United States." Okla. Stat. tit. 51, § 252(2). As to the nature of the religious belief, the inquiry under the Act is simply whether the belief is "religiously motivated," and the Court should *not* inquire into the belief's centrality. According to the Court in *Smith*:

> It is no more appropriate for judges to determine the "centrality" of religious beliefs before applying a "compelling interest" test in the free exercise field, than it would be for them to determine the "importance" of ideas before applying the "compelling interest" test in the free speech field. What principle of law or logic can be brought to bear to contradict a believer's assertion that a particular act is "central" to his personal faith? Judging the centrality of different religious practices is akin to the unacceptable "business of evaluating the relative merits of differing religious claims." As we reaffirmed only last Term, "[i]t is not within the judicial ken to question the centrality of particular beliefs or practices to a faith, or the validity of particular litigants' interpretations of those creeds." *Hernandez v. Commissioner*, 490 U.S. [680,] 699, 109 S. Ct. 2136, 104 L. Ed. 2d 766 [1989]. Repeatedly and in many different contexts, we have warned that courts must not presume to determine the place of a particular belief in a religion or the plausibility of a religious claim.

Employment Div. v. Smith, 494 U.S. 872, 886-887, 110 S. Ct. 1595 (1990) (citations omitted). Further,

> The guarantee of free exercise is not limited to beliefs which are shared by all of the members of a religious sect. Particularly in this sensitive area, it is not within the judicial function and judicial competence to inquire whether the petitioner or his fellow [adherent] more correctly perceived the commands of their common faith. Courts are not arbiters of scriptural interpretation.

Thomas v. Review Bd. of Ind. Employment Sec. Div., 450 U.S. 707, 715-16 (1981); *see Quaring v. Peterson*, 728 F.2d 1121, 1124-25 (8th Cir.1984), *aff'd by equally divided Court per curiam sub nom. Jensen v. Quaring*, 472 U.S. 478 (1985).

> For purposes of determining whether a person's free exercise of religion has been substantially burdened, the problems with "compulsion" and "centrality" tests, which inquire into whether the person's conduct that is being burdened is compelled by or central to his religion, are the same as those in determining whether conduct is religious. It may require a court to do what it cannot do: assess the demands of religion on its adherents and the importance of particular conduct to the religion.

Barr, 295 S.W.3d at 301. Thus, the centrality of Ms. Beach's religious beliefs are not at issue – only whether her religious beliefs are religiously motivated and have been substantially burdened.

Ms. Beach's religion proscribes her from being enrolled in the international system of identification based on her biometrics (*i.e.*, the number or measurement of her body). She is forbidden by her sincerely held religious beliefs to allow a high-resolution facial photograph, or facial biometric, or other biometrics, in a format compliant with international standards, to be captured by DPS. Statement of Undisputed Material Facts ("SUMF") #16. Ms. Beach has learned and believes that the interoperability and open architecture format for the high-resolution biometric facial photograph used by motor license agents as required by DPS to take the photographs for driver's licenses is an internationally set format determined by the United Nations' International Civil Aviation Organization ("ICAO") intended to be "interoperable," and that the database into which her facial biometric data is placed is managed and accessed by a self-described international organization called the American Association of Motor Vehicle Administrators ("AAMVA") and/or its member jurisdictions and corporate entities. SUMF #17. The State has admitted it follows the

AAMVA standards for biometric capture and storage. *Id.* The State also admitted it has no role, function or input in the establishment of the standard for the resolution and format of the biometric information collected driver license applicants, and reemphasized the State "follows the American Association of Motor Vehicle Administrator standards." SUMF #18.

The State identified "MorphoTrust USA" as an entity that has access to the database in which Drivers License and Identification Card Applicants' biometric data is stored, and that "MorphoTrust USA" provides the management, maintenance, hardware, software, logistical support, or any other type of support regarding the databases in which said biometric information is stored. SUMF #19. Further, the State identified "[t]he L-1 Contract" as the contract between the State and another entity regarding the collection, storage, use, sharing or access of the biometric information of driver license applicants. SUMF #20.

Indisputable facts concerning the entity controlling the biometrics database support Ms. Beach's concerns. "MorphoTrust USA, Inc. was formed when L-1 Identity Solutions was acquired in July 2011 by Safran, a global technology powerhouse in aerospace, defense, and security and an international top-tier supplier of systems and equipment. MorphoTrust is a Morpho company and part of Safran Group." SUMF #21. Indeed, MorphoTrust/L-1/Safran Group provides driver license and digital identification services to Latvia, Costa Rica, Mexico, and Ghana, to name a few. *Id.* Safran is based in France. According to its website, "Safran is a global group, with operations on five continents," including significant operations in China and Russia. SUMF #21. According to L-1, now MorphoTrust: "Recognizing the development of standards is crucial to the mass adoption of biometrics, L-1 Identity Solutions actively participates in both nationally-and

internationally- recognized standards initiatives." SUMF #23.

Ms. Beach's religiously motivated practice is abstaining from allowing her biometric information to be captured, placed into a database linked with other entities and jurisdictions in an international system of identification she believes manifests certain Biblical prophecies and prohibitions. SUMF #24. Ms. Beach's religiously motivated practice is based on her sincerely held religious beliefs that the Bible, specifically Revelations 13: 16-18 and 14:9-11, explicitly commands believers to not participate in a global numbering identification system using the number of man, and eternally condemns participation in that system. SUMF #25. While the centrality of the religious beliefs are not to be considered by the Courts, *Smith*, 494 U.S. at 886-887; *Barr*, 295 S.W.3d at 301, Ms. Beach's religious beliefs are sincerely held, an indisputable fact, even acknowledged by her pastor. Put simply, "bio" means "body" and "metric" means "measurement." Hence, a biometric is the number of the body of man, which Ms. Beach believes Revelations explicitly forbids her from submitting into the international and interoperable system described above. SUMF #26.

B. The State's Denial of Ms. Beach's Requested Religious Accommodation Inhibits and Curtails Her Religiously Motivated Practice.

"Under the proper analysis, a burden upon religion exists when "the state conditions receipt of an important benefit upon conduct proscribed by a religious faith, thereby putting substantial pressure on an adherent to modify his behavior and to violate his beliefs." *Quaring*, 728 F.2d at 1125 (quoting *Thomas*. 450 U.S. at 717-18). As in *Quaring*, "[b]y requiring [Ms. Beach] to comply with the photograph requirement, the state places an

unmistakable burden upon her exercise of her religious beliefs." *Quaring*, 728 F.2d at 1125. Like *Quaring*, the State's refusal to accommodate Ms. Beach's religious belief by refusing to issue a driver's license imposes "a condition that would violate a fundamental precept of her religion. Moreover, in refusing to issue [Ms. Beach] a driver's license, the state withholds from her an important benefit." *Id.*

"[A] government action or regulation creates a 'substantial burden' on a religious exercise if it *truly pressures the adherent to significantly modify his religious behavior and significantly violate his religious beliefs*." *Adkins v. Kaspar*, 393 F.3d 559, 570 (5th Cir. 2004) (emphasis added). Hence, "a regulation's effect is 'substantial' when it either (1) influences the adherent to act in a way that violates his religious beliefs or (2) forces the adherent to choose between, on the one hand, enjoying some generally available, non-trivial benefit, and on the other hand, following his religious beliefs." *A.A. v. Needville Indep. Sch. Dist.*, 611 F.3d 248, 264 (5th Cir.2010) (citing *Adkins*, 393 F.3d at 570).

Another proposed definition, recognized by the *Barr* Court in a RFRA case, is as follows: "A person's religious exercise has been substantially burdened under the Texas RFRA when his ability to express adherence to his faith through a particular religiously-motivated act has been meaningfully curtailed *or he has otherwise been truly pressured significantly to modify his conduct*." *Barr*, 295 S.W.3d at 302 (quoting Brief of the American Center for Law and Justice (ACLJ), the American Civil Liberties Union Foundation of Texas (ACLU), Senator David Sibley, and Representative Scott Hochberg as Amici Curiae Supporting Petitioners at 3) (emphasis added). A regulation or law substantially burdens one's free exercise if it prescribes or proscribes conduct the

claimant's religion prescribes or proscribes. *See Smith*, 494 U.S. at 879, 110 S. Ct. at 1600. In this inquiry, "the focus is on the degree to which a person's religious conduct is curtailed and the resulting impact on his religious expression. *The burden must be measured, of course, from the person's perspective, not from the government's.*" *Barr*, 295 S.W.3d at 301 (emphasis added).

Ms. Beach has requested an accommodation on several occasions based on her religious beliefs that she be allowed to submit a low resolution non-biometric photograph in order obtain a driver license. *See* SUMF ## 5-10, 13. The State has denied her request for a religious accommodation. *Id.*

The State's denial has inhibited and curtailed her religiously motivated practice such that she must choose between adhering to her religious beliefs and suffering real consequences or violating her religious beliefs and obtaining a valid driver license. Because she has chosen to adhere to her religious beliefs, she has encountered numerous problems, for example: she is unable to lawfully drive a motor vehicle and in fact was criminally charged for driving without a valid driver's license; she has been denied the ability to acquire prescription medication; she has been denied the ability to use her debit card; she has been denied the ability to rent a hotel room; and, she has been denied the ability to obtain a P.O. box. SUMF # 15.

In *Sherbert v. Verner*, 374 U.S. 398 (1963), the state of South Carolina denied unemployment compensation to a Seventh-day Adventist because she declined to seek work on Saturday, her Sabbath. The Court held that the denial unconstitutionally infringed upon her free exercise of religion because she was required to forego the exercise of her

faith in order to obtain a government benefit to which she was otherwise entitled. In the words of the Court:

> Here, not only is it apparent that appellant's declared ineligibility for benefits derives solely from the practice of her religion, but the pressure upon her to forego that practice is unmistakable. The [lower court] ruling forces her to choose between following the precepts of her religion and forfeiting benefits, on the one hand, and abandoning one of the precepts of her religion in order to accept work, on the other hand. Governmental imposition of such a choice puts the same kind of burden upon the free exercise of religion as would a fine imposed against appellant for her Saturday worship.

Id. at 404. The *Sherbert* Court's ruling has since been applied by other Court's to cases regarding religious objections to driver license photo requirements. *See Quaring*, 728 F.2d at 1125; *BMV v. Pentecostal House of Prayer*, 380 N.E.2d 1225, 1229, 269 Ind. 361, 368 (Ind.1978).

In this case, the State's denial effectively forces Ms. Beach to submit her body to measurement by the State, an even more intrusive burden than one aimed at activities or use of an item. *See A.A.*, 611 F.3d at 266 ("state action in the form of rules regarding hair "directly regulate a part of A.A.'s body and not just a personal effect--like a knife or a rosary--the burden on A.A.'s religious expression is arguably even more intrusive.").

Here, there can be no question Ms. Beach's religiously motivated belief has been substantially burdened. She is "truly pressure[d]" to significantly modify her religious behavior and significantly violate her religious beliefs." *Adkins*, 393 F.3d at 570. The State's denial has (1) influenced her to act in a way that violates her religious beliefs and has forced her to choose between, on the one hand, enjoying some generally available, non-trivial benefit – a license to drive a vehicle and a state issued identification card regularly required in modern life, and on the other hand, following her religious beliefs.

A.A., 611 F.3d at 264. Further, her ability to express adherence to her faith through a particular religiously-motivated act has been meaningfully curtailed and she has otherwise been truly pressured significantly to modify her conduct. *Barr*, 295 S.W.3d at 302.

Photo requirements for licences have been held to constitute a burden on religious practice. *See Quaring v. Peterson*, 728 F.2d 1121, 1125 (8th Cir.1984), *aff'd by equaly divided Court per curiam sub nom. Jensen v. Quaring*, 472 U.S. 478 (1985), discussed *supra*.[4]; *BMV v. Pentecostal House of Prayer*, 380 N.E.2d 1225, 1228, 269 Ind. 361, 367 (Ind.1978) ("Clearly, the photograph requirement has placed the appellees in a dilemma requiring to choose between violating an important religious principle or surrendering their driving privileges").

B. The State Cannot Demonstrate With Clear and Convincing Evidence that its Denial is Essential to Further a Compelling State Interest.

The ORFA "requires the Government to demonstrate that the compelling interest

---

[4]*Alexander v. Trustees of Boston Univ.*, 766 F.2d 630, 644 (1st Cir.1985) (distinguishing the case before it regarding financial aid applications from *Quaring v. Peterson* regarding license photos, describing *Quaring* as a "case where the government seeks to extract information which, by itself, directly violates a religious tenet"). In *Dennis v. Charnes*, 805 F.2d 339 (10th Cir.1984), the Tenth Circuit overruled the trial court's granting of the State's Motion to Dismiss and remanded. In *Dennis*, the plaintiff claimed that the State's refusal to accommodate his religious objection to license photo requirements violated his free exercise rights. Upon remand, the Trial Court found the State's refusal substantially violated the plaintiff's religious free exercise, stating "the higher values of the First Amendment should prevail over the state's concerns about bureaucratic inconvenience." *Dennis v. Charnes*, 646 F. Supp. 158, 164 (D.Colo.1986). The Tenth Circuit and the *Charnes* Trial Court relied heavily on the Eighth Circuit's *Quaring* decision and the United States Supreme Court's affirmation thereof. In *Shrum v. Coweta*, 449 F.3d 1132, 1144-45 (10th Cir.2006), the Tenth Circuit described the *Quaring* case as one where "the Free Exercise Clause has been applied . . . when government officials interfered with religious exercise not out of hostility or prejudice, but for secular reasons, such as . . . facilitating traffic law enforcement." *See State v. Swartzentruber*, 52 Ohio Misc. 2d 1, *4; 556 N.E.2d 531, 534 (Ohio Mun. Ct.1989) (citing *Quaring* with approval, and stating: "It is hard to imagine pressure more substantial than loss of income, *or, in a society where transportation is essential to obtain goods and services, the ability to move about*" (emphasis added)).

test is satisfied through application of the challenged law 'to the person' -- the particular claimant whose sincere exercise of religion is being substantially burdened." *Gonzales*, 546 U.S. at 430-431, 126 S. Ct. 1211 (2006). To do so, courts must "look[] beyond broadly formulated interests justifying the general applicability of government mandates and scrutinize[] the asserted harm of granting specific exemptions to particular religious claimants." *Id.* at 431. The analysis requires that "courts should strike sensible balances, pursuant to a compelling interest test that requires the Government to address the particular practice at issue." *Id.* at 439. The State's "invocation of general interests, standing alone, is not enough--a showing must be made with respect to the 'particular practice' at issue. *A.A.*, 611 F.3d at 268 (quoting *Barr*, 295 S.W.3d at 306).

"A court 'must searchingly examine the interests that the State seeks to promote . . . and the impediment to those objectives that would flow from recognizing the claimed . . . exemption.'" *Id.* (quoting *Yoder*, 406 U.S. at 213, 221). For the State to prevail, then, it cannot rely on "general platitudes," but "must show by specific evidence that the adherent's religious practices jeopardize its stated interests." *Id.* (quoting *Merced*, 577 F.3d at 592). Again, pursuant to ORFA, the State's burden is one of clear and convincing evidence.

In BMV v. Pentecostal House of Prayer, 380 N.E.2d 1225, 1228, 269 Ind. 361, 367 (Ind.1978), the Indiana Supreme Court affirmed the trial Court's ruling that Indiana's statute requiring photos of license applicants was unconstitutional as applied to plaintiffs and in violation of the plaintiffs' free exercise rights. On appeal, the State had argued "that driving an automobile in this state is a privilege subject to regulation under the police power of the

state and that the photograph requirement 'for the purpose of identification' is a reasonable regulation which supersedes the appellees' religious freedoms." *Id.* at 1227, 269 Ind. at 363-64. The appellate Court rejected this argument, holding that the Constitutional right not to have one's photo taken by the State over a religious objection "may be overbalanced only by those governmental interests 'of the highest order and those not otherwise served.'" *Id.* at 1227, 269 Ind. at 365 (quoting *Wisconsin v. Yoder*, 406 U.S. 205, 215, 92 S.Ct. 1526, 1533, 32 L.Ed.2d 15, 25 (1972)). The Court flatly rejected the State's argument that since driving is a privilege, not a right, "no First Amendment problem is raised where a citizens free exercise right is brought into conflict with a mere privilege." *Id.* at 1229, 269 Ind. at 368 (applying *Sherbert*, 374 U.S. 404, 83 S.Ct. 1794).

The Court rejected the State's asserted interests in the photo requirement, *i.e.*, ensuring competency of drivers and identification, holding that there "are other alternatives available to the Bureau which would satisfy this purpose without impinging on the rights of these appellees." *Id.* at 1229, 269 Ind. at 369. On the other hand, when a *convicted felon* objected to photo requirements in his booking process, the State's interests outweighed the felon's religious free exercise rights. *United States v. Slabaugh*, 852 F.2d 1081 (8th Cir.1988). The importance of the distinction between *Pentecostal House of Prayer* and *Slabaugh* must not be overlooked.

As stated in 47 O.S §6-101(C), the State's purpose for driver licenses is so that a person "may exercise the privilege thereby granted upon all streets and highways in this state." In fact, individuals are forbidden to drive without a license. *Id.* at §6-101(A). According to 43 O.S. §6-110.2(A), the State requires all applicants for a driver license or

identification card to submit to finger imaging "*for the purposes* of proof of identity and to ensure the security of the driver license or identification card issued to the applicant." In other words, the purpose for driver's licenses is driving. The State's purpose for the identification requirements in the application process is proof of identification and the integrity of the issued license. The State's purpose for refusing the religious accommodation requested by Ms. Beach is another matter, as the proper analysis focuses on the State's asserted interest in denying the requested accommodation, *not* on the asserted interest in the underlying requirement. Okla. Stat. tit. 51, § 253; *see Gonzales*, 546 U.S. at 431. Further, the State's denial has placed substantial burdens of Ms. Beach well outside the realm of its statutory purpose for driver licenses, i.e., ability to drive and proof of identification to the State and card integrity – she has been denied the ability to acquire prescription medication; the ability to use her debit card; the ability to rent a hotel room; and, the ability to obtain a P.O. box. SUMF # 15.

Thus far, the State's sole asserted purpose for its refusal to provide a religious accommodation to Ms. Beach is that "[a]llowing exceptions would open the door for unlimited requests for exceptions and defeat the purpose of having such stringent identity verification measures. Religion does not play a role in this process." SUMF #28. Further, "[t]he purpose for collecting biometric images is to verify that the person applying for a DL/ID card is that person." *Id.* When asked in Discovery to provide copies of any document containing the State's asserted purposes for the denial or from which the purposes were derived in whole or in part, the Stated answered under oath, "No documents to produce." SUMF #29. Thus, there is *no* evidence supporting the State's assertion. To be clear,

> A state's interest in avoiding an administrative burden becomes compelling only when it presents administrative problems of such magnitude as to render the entire statutory scheme unworkable. *See Sherbert v. Verner*, supra, 374 U.S. at 408-09. The record contains no evidence, however, that allowing religious exemptions to the photograph requirement will jeopardize the state's interest in administrative efficiency.

Quaring, 728 F.2d at 1127.

In its Answer, the State's sole asserted compelling governmental interest in refusing to provide an accommodation to Ms. Beach on account of her sincerely held religious beliefs and religiously motivated practice is that "[t]he State of Oklahoma is required by Federal law to gather biometric data as part of its motor vehicle licensing process and there is a compelling governmental interest in complying with the applicable Federal laws." SUMF #30. In fact, there is no federal law requiring the State to gather biometric data as part of its motor licensing process, *as the State now admits*. SUMF #31.

In short, the State has failed to set forth anything other than an "invocation of general interests," which, "standing alone, is not enough." *A.A.*, 611 F.3d at 268 (quoting *Barr*, 295 S.W.3d at 306). Again, this Court must "look[] beyond broadly formulated interests justifying the general applicability of government mandates" – like the State has asserted here, "and scrutinize[] the asserted harm of granting specific exemptions to particular religious claimants." *Gonzales*, 546 U.S. at 431, 126 S. Ct. 1211 (2006).

There is no specific, let alone clear and convincing, evidence of "the interests that the State seeks to promote . . . and the impediment to those objectives that would flow from recognizing the claimed . . . exemption.'" *A.A.*, 611 F.3d at 268 (quoting *Yoder*, 406 U.S. at 213, 221). The State's reliance on "general platitudes," *id.*, like those it has asserted, is not enough. Ms. Beach is entitled to summary judgment as a matter of law that

the State's denial of her requested religious accommodation is not essential to further a compelling state interest.

C. The State Cannot Demonstrate With Clear and Convincing Evidence that its Denial is the Least Restrictive Means of Furthering that Compelling State Interest.

Even if the State successfully demonstrated with clear and convincing evidence that its denial was essential to further a compelling state interest, it still must demonstrate its denial is the least restrictive means of furthering that interest. The Court need only consider this step if it concludes the State has demonstrated a compelling interest in denying Ms. Beach's requested religious accommodation.

The State asserts "[t]here are no less restrictive means used by the Department that would verify identity to that level of certainty and with the same degree of security," than requiring DL/ID card applicants to submit biometric information. SUMF #35. *No documentation has been provided by the State to support this assertion.*

On the other hand, the State admits "there are other ways to confirm identity" than to require DL/ID applicants to submit biometric information. SUMF #32. The State admits "that an individual's birth certificate is considered a primary form of ID. Applicants must also provide a secondary form of ID." SUMF #33.[5] Ms. Beach has a birth certificate – *which*

[5]According to the DPS website, satisfactory "secondary proof of identification" documents include: Photo identification card issued by one of the following: Oklahoma public, private, or parochial secondary school; Oklahoma institution of higher education; Oklahoma technology center school; Oklahoma employer; or, Oklahoma gun permit; Pilot license; Oklahoma lifetime hunting or fishing license; Oklahoma voter identification card; Social Security card; Health insurance card; Motor vehicle registration or title; Marriage certificate; Separation or divorce judgment; High school, technology center school, college, or university diploma; Professional degree, certificate, or license; Deed or title to property in Oklahoma, including a burial plot deed; Health, life, or home insurance policy issued to the applicant; and, Automobile insurance policy or security verification form issued to the applicant.

has previously been accepted as a primary form of identification by DPS and the tag agent and she has secondary forms of ID to satisfy the non-objectionable identification requirements. SUMF #34. The State's unsupported assertion that Ms. Beach's identification cannot be ascertained to a sufficient degree of certainty unless she submits biometric information is baseless and absurd.

As in *Pentecostal House of Prayer*, "there are other alternatives available to the [State] which would satisfy this purpose without impinging on the rights of" Ms. Beach, *id.* at 369, 380 N.E.2d at 1229, and it is the State's burden to prove otherwise by clear and convincing evidence. The State has not demonstrated or even indicated that any of its cameras currently used to take applicant photographs cannot be formatted to take a low-resolution non-biometric photograph and save the image to the database. Another alternative would be that the State could acquire a single low-resolution camera to be located at DPS headquarters for use when an applicant requests a religious accommodation to the biometric facial photo.

Further, an applicant could take the primary and secondary ID documents presented at the driver license examiner's office to the tag agent to prove his or her identity. This would prove the applicant who took the test at the examiner's office is the same person who is present at the tag agent to receive the card.

Yet another alternative would be that the religious accommodation applicant could be required first to go to the tag agent with primary and secondary identification and obtain an identification card with a low-resolution photo and no fingerprints. The applicant would then take that card to the examiner's office and take the test. After successfully completing the test, the applicant would return to the tag agent with the ID card and papers. The State

could also issue a driver license to Ms. Beach with no photograph at all, as several other States allow those with religious objections to photographs, such as Illinois, Indiana, and Kentucky.

The bottom line is that there are multiple ways the State could accommodate the religious beliefs of applicants like Ms. Beach while still satisfying its stated purpose and interest in verifying the applicant's identification at each stage of the process. This is especially true given that biometrics do not "prove" a person's identity – the "breeder documents", e.g., birth certificates, do. SUMF #36. The biometrics simply attempt to tie the person to the breeder document. There are less restrictive means available to the State to accomplish its purpose in a manner that does not substantially burden Ms. Beach's religious free exercise. The State cannot demonstrate to the contrary with clear and convincing evidence.

V. CONCLUSION

Ms. Beach has established that her religiously motivated practice has been substantially burdened, *i.e.*, inhibited or curtailed, by the State. The State has not and cannot satisfy its burden to demonstrate with clear and convincing evidence that its denial of Ms. Beach's requested religious accommodation is essential to further a compelling governmental interest; *and* the least restrictive means of furthering that compelling governmental interest. The State has therefore violated the Oklahoma Religious Freedom Act, Okla. Stat. tit. 51, § 253, and pursuant to the Act, Okla. Stat. tit. 51, § 256, Ms. Beach is entitled to declaratory relief, a judgment for monetary damages, and reasonable costs and attorney fees.

Ms. Beach respectfully requests this Honorable Court to grant her Motion for

Summary Judgment as to Count I of her Petition, and enter:

a. A declaratory judgment that pursuant to the Oklahoma Religious Freedom Act, Ms. Beach's free exercise of religion is substantially burdened by the State's refusal to accommodate her sincerely held religious beliefs and religiously motivated practice;

b. A declaratory judgment that the State's requirement and refusal to provide an accommodation to Ms. Beach is not essential to further a compelling governmental interest;

c. A declaratory judgment that even if the State's requirement and refusal to provide an exemption to Ms. Beach was essential to further a compelling governmental interest, the requirement and refusal to provide an accommodation to Ms. Beach is not the least restrictive means of furthering that compelling governmental interest;

d. A declaratory judgment that in order to comply with the Oklahoma Religious Freedom Act, the State must provide an accommodation to Ms. Beach, on account of her sincerely held religious beliefs and religiously motivated practice, which allows her to submit a low-resolution non-biometric facial photograph in order to apply for and obtain a driver's license, and apply for and obtain a driver's license without the capture of her fingerprint biometrics;

e. A permanent injunction enjoining the State from denying Ms. Beach a driver's license without providing an accommodation to her on account of her sincerely held religious beliefs and religiously motivated practice, which allows her to submit a low-resolution non-biometric facial photograph which is not stored in any database in order to apply for and obtain a driver's license, and apply for and obtain a driver's license without the capture of her fingerprint biometrics;

f. A judgment awarding monetary damages as specifically authorized by Okla. Stat. tit. 51, § 256(B) in excess of $10,000.00;

g. An award of reasonable costs and attorney fees, as specifically authorized by Okla. Stat. tit. 51, § 256(B); and,

h. An Order granting and awarding such other and further relief to which Plaintiff may be entitled and which this Court deems just and proper.

Upon granting this Motion, Ms. Beach prays the Court set a hearing to determine the appropriate Order of Declaratory Judgment and a hearing on the appropriate money judgment and attorney fees and costs.

Respectfully submitted,

M. EILEEN ECHOLS, OBA #2607
BENJAMIN P. SISNEY, OBA #21816
ECHOLS & ASSOCIATES
9925 South Pennsylvania, Suite 100
Oklahoma City, Oklahoma 73159
Telephone: (405) 691-2648
Fax: (405) 691-5648
Attorneys for Plaintiff

DOUGLAS R. MCKUSICK
(douglasm@rutherford.org)
Virginia State Bar No. 72201
THE RUTHERFORD INSTITUTE
P.O. Box 7482
Charlottesville, VA 22906-7482
Telephone: (434) 978-3888
Fax: (434) 978-1789
Attorney for Plaintiff

VERIFICATION

STATE OF OKLAHOMA)
) ss.
COUNTY OF CLEVELAND)

KAYE BEACH, being first duly sworn upon his oath, states:

That she is the Plaintiff above named; that she has read the above and foregoing document and knows the contents thereof, and that the statements, allegations and facts therein set forth are true and correct to the best of her information, knowledge and belief.

Kaye Beach
KAYE BEACH
Plaintiff

Subscribed and sworn to before me this 17th day of June, 2013.

Michele Bradley
Notary Public

My Commission Expires:

(SEAL)

MICHELE BRADLEY
Notary Public
State of Oklahoma
Commission # 11000698 Expires 01/28/15

CERTIFICATE OF SERVICE

This is to certify that on the 19th day of June, 2013, a true and correct copy of the above and foregoing document was mailed, postage prepaid thereon, to:

JOHN D. HADDEN, ESQ.
KEVIN L. MCCLURE, ESQ.
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N.E. 21st Street
Oklahoma City, Oklahoma 73105
Telephone: (405) 521-4274
Fax: (405) 521-4518
Attorneys for Defendants Department of Public Safety, Thompson and Adams

DOUGLAS R. MCKUSICK, ESQ.
The Rutherford Institute
1440 Sachem Place
Charlottesville, VA 22901
Attorney for Plaintiff

BENJAMIN P. SISNEY

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1483

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 1

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Case No. CJ-2011-1469**
	)	
OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,	)	
	)	
Defendants.	)	

PLAINTIFF KAYE BEACH'S SWORN AFFIDAVIT PURSUANT TO 12 O.S. §2056(E)

I am Kaye Beach, the Plaintiff in the above captioned and numbered case. I have personal knowledge of the facts set out herein, and I am of due age and competency to testify on the matters stated herein. The statements, allegations and facts herein set forth are true and correct to the best of my information, knowledge and belief.

1. I am a resident of the State of Oklahoma and of Cleveland County, Oklahoma.

2. On March 8, 2011, I attempted to apply for a renewal driver's license at Fusion Tag Agency (the "Tag Agency") located at1236 North Interstate Drive, Norman, OK 73072, in Cleveland County, Oklahoma.

3. Notwithstanding my satisfaction or ability to satisfy any other relevant requirements for obtaining a renewal driver's license, my attempt to apply was rejected by the Tag Agency.

4. The Tag Agent informed me it was required by law to take a high-resolution digital facial photograph, and that I could not apply for or obtain a renewal license without allowing

the DPS agent to capture her biometric facial photograph or fingerprints.

5. I requested and was denied an accommodation on account of my sincerely held religious beliefs and religiously motivated practice, which are more fully set forth below.

6. Later that same day, March 8, 2011, I contacted DPS directly and again explained my religious objection and requested an accommodation. On or about March 11, 2011, I followed up by telephone and was informed by a DPS employee, Mr. Steve Grunyard, that the biometrics were required by law and that there would be no accommodation or alternative.

7. On March 18, 2011, I sent a letter to DPS identifying my religious objections and requesting an accommodation. I informed DPS that I does not object to a low-resolution facial photograph. I also specifically asked, "Are there any available administrative remedies that I can pursue that I have not pursued to this point or have I exhausted all administrative remedies."

8. On April 27, 2011, she received an email from Stephen J. Krise, General Counsel, Oklahoma Department of Public Safety, stating as follows:

> I'm sorry I missed your call, but I have obtained information related to your question of whether there is an alternative to having a driver license photograph that does not capture facial recognition features, commonly referred to as biometric data. Such photographs are required by statute and the law does not provide for an alternative or exemption.

9. On June 5, 2011, I received a criminal citation for a violation described as "EXPIRED DRIVER'S LICENSE, with a notation identifying Norman Municipal Code Section 20-509(a), entitled "Driving: License of driver." This municipal ordinance, in pertinent part, provides that "[n]o person shall operate any vehicle upon the streets of the City without that person being licensed in the manner now required by the laws of the State of Oklahoma, which are hereby incorporated into the Code of the City of Norman as if fully set out in this subsection." Norman Municipal Code, Sec. 20-509(a).

10. On July 18, 2011,I again attempted to obtain a renewal driver's license at Fusion Tag Agency in Norman, Oklahoma, and was again denied on account of my religiously motivated inability to allow the Tag Agent to capture my biometrics.

11. On July 21, 2011, I appeared with counsel at the Norman Municipal Courthouse for my arraignment, where a Norman Assistant City Attorney dismissed the charge.

12. As a result of the State's refusal to provide an accommodation, I am unable to lawfully drive a motor vehicle and in fact was criminally charged for driving without a valid driver's license; I have been denied the ability to acquire prescription medication; I have been denied the ability to use my debit card; I have been denied the ability to rent a hotel

room; and I have been denied the ability to obtain a P.O. box. This is so even though I have a other forms of identification.

13. I am forbidden by my sincerely held religious beliefs to allow a high-resolution facial photograph, or facial biometric, or other biometrics, in a format compliant with international standards, to be captured by the State.

14. I have learned that the interoperability and open architecture format for the high-resolution biometric facial photograph used by motor license agents as required by DPS to take the photographs for driver's licenses is an internationally set format determined by the United Nations' International Civil Aviation Organization ("ICAO") intended to be "interoperable," and that the database into which my facial biometric data would be placed is managed and accessed by a self-described international organization called the American Association of Motor Vehicle Administrators ("AAMVA") and/or its member jurisdictions and corporate entities.

Regarding the ICAO, "the International Civil Aviation Organization serves as the global forum for its ***191 Member States [i.e. nations]***." ICAO website, "About ICAO," at http://www.icao.int/Pages/default.aspx (emphasis added), attached as Exhibit A.

> With the collaboration of Member States, ICAO plays an essential leadership role in the field of aviation security with the ultimate goal of enhancing civil aviation security worldwide. To this end, its efforts are focused primarily on developing and coordinating an effective global policy and legal framework in response to the evolving threat to civil aviation, conducting audits that identify aviation security shortcomings, ***and assisting States in implementing security Standards and resolving deficiencies***.

Id. at http://www.icao.int/Security/Pages/default.aspx (emphasis added), attached as Exhibit B. The ICAO standard for biometric images was adopted in the REAL ID ACT OF 2005 for use by Sate DMVs in capturing biometric images from driver license applicants. *See* American Center for Law and Justice Letter to Oklahoma Representative Charles Key, January 31, 2008, at 4, attached as Exhibit C. ("REAL ID also complies with certain technical requirements set by the United Nations' International Civil Aviation Organization ("ICAO")). According to the ACLJ, REAL ID "requirements comply with internationally accepted standards for ID cards" regarding "universal interoperability" and "biometrics," *Id.* at 1, and the "REAL ID system is being engineered to be interoperable worldwide. [The Department of Homeland Security] has clearly indicated its intentions to share U.S. Citizens' biometric and other data with other nations, international organizations, and security corporations, and indeed has already implemented such programs." *Id.* at 4. The ACLJ also expressed its concern that "the personal information and biometric data of common citizens will be incorporated into this system" and cautioned against "the impact of the interoperability of data and databases worldwide combined with international trends in data collection." *Id.* at 1.

The American Civil Liberties Union (ACLU) and the American Center for Law and Justice (ACLJ) united to express their concerns at a National Press Club event. Available at: http://www.youtube.com/watch?v=JwgVeXx22fI.

Regarding AAMVA, according to its website:

> The American Association of Motor Vehicle Administrators (AAMVA) is a tax-exempt, nonprofit organization developing model programs in motor vehicle administration, law enforcement and highway safety. The association also serves as an information clearinghouse in these areas, and acts as the international spokesman for these interests. . . . AAMVA's membership includes associations, organizations and businesses that share an interest in the association's goals

AAMVA, "About AAMVA," at http://www.aamva.org/about-aamva/, attached as Exhibit D. Further, "AAMVA's programs encourage uniformity and reciprocity among the states and provinces." *Id.* "AAMVA's membership includes associations, organizations and businesses that share an interest in the association's goals." *Id.* "Key among AAMVA's goals is improving highway safety and identification security by promoting uniform standards for all areas related to driver licensing." AAMVA website, at http://www.aamva.org/Driver-Licensing-Identification/, attached as Exhibit E.

> The DL/ID Card Design Standard (CDS) was developed by the Card Design Standard committee made up of jurisdictional and federal government members. The CDS provides for the design of driver licenses (DL) and identification (ID) cards and ***its intent is to improve the security of the DL/ID cards and the level of interoperability among cards issued by all North American jurisdictions***.

Id. at http://www.aamva.org/DL-ID-Card-Design-Standard/ (emphasis added), attached as Exhibit F. The DL/ID Card Design Standard Committee Roster includes representatives from Ontario, British Columbia, and Quebec. *Id.* at http://www.aamva.org/Card-Design-Standards-Committee/, attached as Exhibit G. The American Center for Law and Justice has also recognized AAMVA's status as an "international organization," and its goal of establishing a uniform North American driver license/ID card. *See* American Center for Law and Justice Letter to Oklahoma Representative Charles Key, January 31, 2008, at 4, attached as Exhibit C.

15. According to the International Biometrics and Identification Association (IBIA):

> **Biometrics - Physical & Behaviorally-Based Identity Authentication**
>
> Instead of basing identity authentication on what someone possesses or what someone knows, biometric identification is based on what one is, or

how one behaves, ***This approach to identification is made possible by technology developments that enable precise measurement coupled with computational power that allows measurements to be transformed into mathematical representations that can be rapidly compared.***

The Unique Physical Attribute

Fingerprints on cards, and lifted from the scene of a crime have been used for more than one hundred years as proof of individual identification for forensic and law enforcement purposes. Once time-consumingly collected as inked sets on cards, they are now routinely collected by electronic or optical sensors that turn patterns once only defined as whorls and arches into mathematical representations called biometric templates. ***Other physical attributes that can be measured and converted into mathematical representations include: faces, fingerprints, hands, iris patterns, retinal patterns***, vein patterns, voice patterns, and DNA. Exploratory work has been done to establish whether physical characteristics such as earlobes and body odor can be effectively measured, mathematically represented, and rapidly compared for use in electronic identity authentication.

International Biometrics and Identification Association, http://www.ibia.org/biometrics/background/ (emphasis added), attached as Exhibit H. Specifically regarding biometric facial images:

> The relationships between the parts of the face, its curves and contours, remain relatively stable from childhood onward. Facial recognition techniques use this stability as their point of departure. Facial recognition technologies utilize digital photographs to create mathematical descriptions of individual faces and then compare them against those stored in a database. Facial recognition requires a large image capture device and clear lighting conditions and is therefore most suitable to authenticate identity at fixed locations, such as facility access points.

Id. at http://www.ibia.org/biometrics/technologies/face, attached as Exhibit I.

The IBIA's "Mission" is stated as follows:

> The International Biometrics & Identification Association (IBIA) is a trade association founded in September 1998 in Washington, DC that promotes the effective and appropriate use of technology to determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.

> Recognizing the vital role identity plays ***in a globally connected world***, IBIA brings stakeholders into a single organization that provides a
> •forum for exchanging information and ideas;
> •clearinghouse for resolving issues and establishing policy;
> •voice for policy advocacy and education;
> •connection to complementary organizations and standards bodies.

Id. at http://www.ibia.org/association/ (emphasis added), attached as Exhibit J. Other supporting documents regarding my religious beliefs and the international and interoperable system (e.g., regarding L-1, MorphoTrust USA, and Safron Group) in which I must not participate are attached as Exhibits 10-12 to my Motion for Summary Judgment and are incorporated herein by reference as if fully set forth herein.

The federal government is sharing biometric information internationally. According to Konrad Trautman, director of intelligence at Special Operations Command, "having the right policies, techniques and procedures in place for partner nations will become vital. '*The policy allows us to lash that together, not just for the domestic intelligence concerns but international policy as well or bi-national policy*,' he said." Magnuson, S., "Defense Department Under Pressure to Share Biometric Data," National Defense Magazine, Jan. 2009, available at http://www.nationaldefensemagazine.org/ARCHIVE/2009/JANUARY/Pages/DefenseDepartmentUnderPressuretoShareBiometricData.aspx (emphasis added), attached as Exhibit K. Al Miller, a consultant to the office of homeland defense and America's security affairs, said that as of 2009, "the *United States has bi-lateral agreements to share biometric data with about 25 countries*. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement." *Id.* (emphasis added).

Indeed, according to a federal government website, the goal is "to encourage greater collaboration and sharing of information on biometric activities among government departments and agencies; commercial entities; *state, regional, and international organizations*; and the general public." Biometric.gov, "Welcome," available at http://www.biometrics.gov/ (emphasis added), attached as Exhibit L.

As outlined in the National Security Presidential Directive 59 and Homeland Security Presidential Directive 24 executed by President Bush in 2008:

> Through integrated processes and interoperable systems, agencies shall, to the fullest extent permitted by law, 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 Secretary of State, in coordination with the Secretaries of Defense and

> Homeland Security, the Attorney General, and the DNI, *shall coordinate the sharing of biometric and associated biographic and contextual information with foreign partners in accordance with applicable law, including international obligations undertaken by the United States.*

NSPD-59 / HSPD-24, June 5, 2008, at ¶¶11, and 17, available at http://www.biometrics.gov/Documents/NSPD59%20HSPD24.pdf (emphasis added), attached as Exhibit M. The FBI already has biometric information sharing relationships with 77 countries. *See* FBI CJIS Staff Paper—Update on Biometric Sharing Program—June 2012, at p. 2, available at https://www.eff.org/document/fbi-cjis-staff-paper%E2%80%94update-biometric-sharing-program%E2%80%94june-2012, attached as Exhibit N.

Bringing my concerns close to home, a number of States are exploring and two States have already entered into agreements with the FBI regarding biometrics sharing and facial recognition programs. According to the FBI, Memoranda of Understandings (MOUs) "have also been executed with Hawaii and Maryland, and South Carolina, Ohio, and New Mexico are engaged in the MOU review process for Facial Recognition Pilot participation. Kansas, Arizona, Tennessee, Nebraska, and Missouri are also interested in Facial Recognition Pilot participation." Jerome M. Pender, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law*, Washington, D.C., July 18, 2012, available at http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties, attached as Exhibit O; see also, Exhibit P, attached hereto, which are copies of Memoranda of Understanding (MOUs) between Hawaii and the FBI and Maryland and the FBI regarding "Interstate Photo System Facial Recognition Pilot."

My inability to knowingly submit my biometrics into an international system of identification and control are at least two-fold: One, the system used by Oklahoma DPS is already part of that system insofar as it is constructed and managed by international entities and pursuant to internationally set standards; and Two, the federal government is already sharing biometric information with other nations and entities, and now other States are already entering into agreements with the federal government to share biometric information. Oklahoma may enter into such an agreement at any time. My religious beliefs prohibit me from allowing my biometrics from being a part of that system.

16. My religiously motivated practice is abstaining from allowing my biometric information to be captured, placed into a database and linked with other entities and jurisdictions in an international system of identification I believe manifests certain Biblical prophecies and prohibitions.

17. I believe that the Bible, specifically Revelations 13: 16-18 and 14:9-11, explicitly commands believers to not participate in a global numbering identification system using the number of man, and eternally condemns participation in that system. I would violate

my religious beliefs by knowingly submitting my biometrics, i.e., the number or measurement of my body, into this system. I am a believer. The cited passages provide as follows:

> Revelations 13:
>
> 16 It also forced all people, great and small, rich and poor, free and slave, to receive a mark on their right hands or on their foreheads, 17 so that they could not buy or sell unless they had the mark, which is the name of the beast or the number of its name. 18 This calls for wisdom. Let the person who has insight calculate the number of the beast, for it is the number of a man.[a] That number is 666.
>
> Revelations 14:
>
> 9 A third angel followed them and said in a loud voice: "If anyone worships the beast and its image and receives its mark on their forehead or on their hand, 10 they, too, will drink the wine of God's fury, which has been poured full strength into the cup of his wrath. They will be tormented with burning sulfur in the presence of the holy angels and of the Lamb. 11 And the smoke of their torment will rise for ever and ever. There will be no rest day or night for those who worship the beast and its image, or for anyone who receives the mark of its name."

Put simply, "bio" means "body" and "metric" means "measurement." Hence, a biometric is the number of the body of man, which I believe Revelations explicitly forbids me from submitting into the international and interoperable system I have described above.

18. The State refuses to provide an accommodation to me which allow me to obtain a driver's license without submitting my biometric information based on my sincerely held religious beliefs and religiously motivated practice.

19. I have a birth certificate which has previously been accepted as a primary form of identification by DPS and the tag agent and I have secondary forms of ID to satisfy the State's non-objectionable identification requirements.

Kaye Beach

KAYE BEACH
Plaintiff

Subscribed and sworn to before me this 17th day of June, 2013.

Michelle Bradley
Notary Public

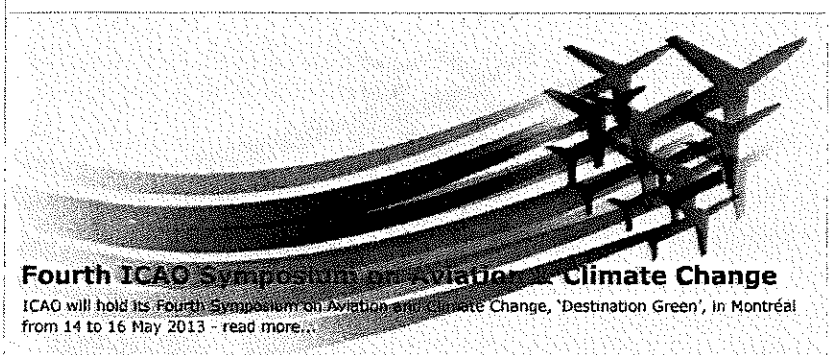
My Commission Expires:

(SEAL) MICHELE BRADLEY
Notary Public
State of Oklahoma
Commission # 11000398 Expires 01/28/15

INTERNATIONAL CIVIL AVIATION ORGANIZATION
A United Nations Specialized Agency

Search this site...

About ICAO | Strategic Objectives | Meetings & Events | Publications | Online Store | Employment



Fourth ICAO Symposium on Aviation and Climate Change

ICAO will hold its Fourth Symposium on Aviation and Climate Change, 'Destination Green', in Montréal from 14 to 16 May 2013 - read more...

38th ICAO Assembly | LPR Technical Seminar | Destination Green | Facts & Figures | Young Aviation Professionals

Latest News

Positions Announced Under New ICAO/IATA/ACI - Young Aviation Professionals Programme | 21/3/2013

Once-A-Decade ICAO Air Transport Conference Convenes | 18/3/2013

See more ...

Recent Events

PIRG-RASG Global Coordination Meeting | ICAO HQ, Montréal, Canada | 19/3/13

Sixth Worldwide Air Transport Conference (ATConf/6) | Montréal, Canada | 17/3/13 - 22/3/13

Next Generation of Aviation Professionals (NGAP) and TRAINAIR PLUS Regional Symposia | Montego Bay, Jamaica | 5/2/13 - 7/2/13

See more ...

About ICAO

Assistance and Cooperation for Globally Sustainable Air Transport
International Civil Aviation Day Theme

Constantly seeking to foster and support the sustainable growth of air transport, the International Civil Aviation Organization serves as the global forum for its 191 Member States. Amongst its many other functions supporting all aspects of international civil aviation, ICAO brings together States and key industry organizations to determine areas of strategic priority, develops policies and standards, coordinates global monitoring, analysis and reporting initiatives, and delivers targeted assistance and capacity building.

Governing Bodies

Assembly

Council

Secretariat

Secretary General

Bureaus

Regional Offices

Highlights

Safety Audits

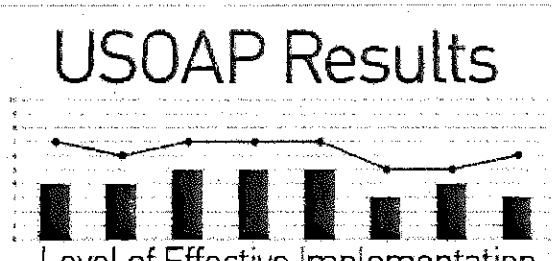
Air Transport Sustainability

Aviation and Tourism

ICAO and EU intensify collaboration

SG Award

McGill/ICAO Air & Space Event



The ICAO Universal Safety Oversight Audit Programme (USOAP) continuously monitors State safety oversight capabilities. For an interactive display of ICAO's States and Regions and their respective USOAP results - please follow this link...

Services & Resources

Carbon Calculator

iSTARS

FITS

ICAO Data+

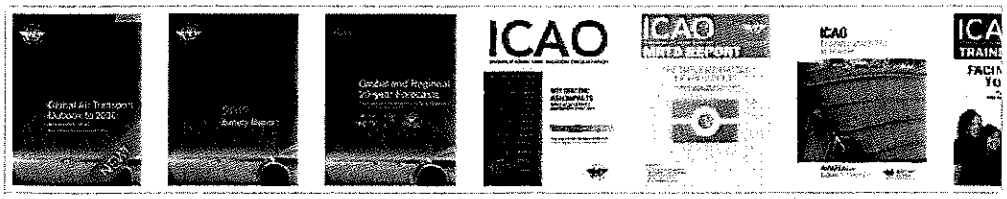
Treaty Collection

Technical Co-operation

Procurement

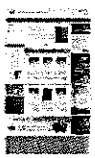
Economic Facts & Figures

Featured Products

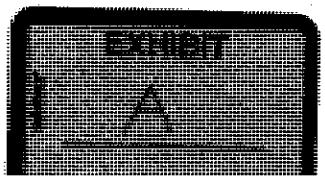


Online Store

Shop for ICAO's aviation products and services.



Go to Store...



Help

Terms & Conditions
Site Index
Links
FAQ
Web Support

Contact Us

Headquarters
Regional Offices

Regional Offices Websites

Asia and Pacific (APAC) Office, Bangkok
Eastern and Southern African (ESAF) Office, Nairobi
European and North Atlantic (EUR/NAT) Office, Paris
Middle East (MID) Office, Cairo
North American, Central American and Caribbean (NACC) Office, Mexico City
South American (SAM) Office, Lima
Western and Central African (WACAF) Office, Dakar

INTERNATIONAL CIVIL AVIATION ORGANIZATION
A United Nations Specialized Agency

Search this site...

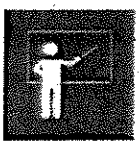
About ICAO | Strategic Objectives | Meetings & Events | Publications | Online Store | Employment

Security

- Aviation Security FAQs
- Aviation Security Policy
- Facilitation
- Implementation Support and Development
- Universal Security Audit
- Machine Readable Travel Documents
- Public Key Directory
- Contact Us

POLICY & REGULATIONS

AUDITS



ASSISTANCE & TRAINING

ICAO > Security

Security

With the collaboration of Member States, ICAO plays an essential leadership role in the field of aviation security with the ultimate goal of enhancing civil aviation security worldwide. To this end, its efforts are focused primarily on developing and coordinating an effective global policy and legal framework in response to the evolving threat to civil aviation, conducting audits that identify aviation security shortcomings, and assisting States in implementing security Standards and resolving deficiencies.

See more ...

Security News

EU/ICAO Collaboration Expands to Include New Security Provisions	18/3/13
Aviation Heavyweights Join Forces on New Young Professionals Programme	10/1/13
Communiqué of the ICAO High-level Conference on Aviation Security	20/9/12
States Forge Stronger, More Sustainable Future for Aviation Security	14/9/12

1 **2** **Next »**

Security Meetings & Events

Ninth Symposium and Exhibition on MRTDs, Biometrics and Border Security	22 - 24/10/13	Montréal, Canada
Assembly - 38th Session of the Assembly	24/09 - 05/10/13	ICAO Headquarters, Montréal, Canada
Legal Committee - 35th Session	06 - 15/05/13	ICAO Headquarters, Montréal, Canada
Twenty-first Meeting of the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD/21)	10 - 12/12/12	ICAO Headquarters, Montréal Canada

1 **2 3 4 5 6 7 8 9 10 Next »**

Help

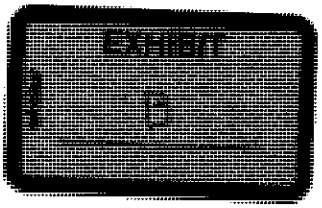
Terms & Conditions
Site Index
Links
FAQ
Web Support

Contact Us

Headquarters
Regional Offices

Regional Offices Websites

Asia and Pacific (APAC) Office, Bangkok
Eastern and Southern African (ESAF) Office, Nairobi
European and North Atlantic (EUR/NAT) Office, Paris
Middle East (MID) Office, Cairo
North American, Central American and Caribbean (NACC) Office, Mexico City
South American (SAM) Office, Lima
Western and Central African (WACAF) Office, Dakar



About AAMVA

Strategic Plan | General Information | Office Hours and Holiday Schedule

2012-2014 Strategic Plan

The AAMVA Board of Directors adopted a three-year strategic plan in the spring of 2011, which sets a course for us to deliver member benefits in a variety of areas. Our staff has been working on an operational plan for FY 2012, which begins October 1, to set priorities and outcomes to achieve the new plan.

A brochure with a summary of the plan goals and an informative powerpoint presentation provides additional detail on the plan's four major goals, significant sub-goals and how we will measure success in each area.

AAMVA Mission

To support North American motor vehicle and law enforcement agencies in achieving their mission.

AAMVA Vision

AAMVA is the valued and trusted organization representing and serving the motor vehicle and law enforcement community across North America.

Download

- Strategic Plan brochure
- Powerpoint Presentation detailing the major goals

Related Content

AAMVA Policy Positions

AAMVA Bylaws

Contact Us

Staff Listing

Biographies & Photos

AAMVA Lexicon (glossary of terms)

Commonly Used Acronyms

Report Legal/Ethical Violations

AAMVA celebrates its 80th anniversary!

ACLJ
American Center
for Law & Justice

January 31, 2008

Representative Charles Key
2300 N. Lincoln Blvd., Room 405
Oklahoma City, OK 73105

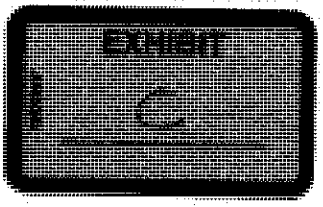
Dear Representative Key:

This letter is in response to your request for information from the American Center for Law & Justice ("ACLJ") regarding the REAL ID Act of 2005 ("REAL ID"). In your letter, you expressed concerns that REAL ID implicated constitutional issues such as state and national sovereignty, individual privacy, and religious freedom. In addition, you expressed concern about the use of biometrics connected to the growing trend of information sharing internationally. While we recognize that many aspects of REAL ID are justifiable in light of the current world situation, the ACLJ's research indicates that there are legitimate causes for concern. As you are aware, REAL ID is the subject of increasing debate as the deadline for state compliance nears. While the issues of privacy and identity theft appear to be the most easily recognized and most commonly discussed, our research has revealed that within REAL ID, there are other issues which merit careful scrutiny. We appreciate your bringing this subject to our attention, and we will continue to monitor these issues as they develop. This letter addresses some preliminary observations.

I. REAL ID: BACKGROUND

The REAL ID Act of 2005 was passed as an amendment to the 2005 Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief. The REAL ID amendment was passed unanimously in the U.S. Senate without debate, and passed overwhelmingly in the U.S. House of Representatives with limited debate. The Act prohibits any federal agency from "accept[ing], for any official purpose, a driver's license or identification card issued by the State to any person unless the State" meets certain requirements. These requirements comply with internationally accepted standards for ID cards: anti-fraud features, universal "interoperability" via machine-readable technology, biometric data, and a linked electronic database operated by an international organization containing all such information. The Final Rule for implementation of REAL ID has been issued, which specifies May 11, 2008 as the effective date for REAL ID.

201 Maryland Avenue, N.E.
Washington, DC 20002
202-546-8890



If a state does not comply and does not formally request an extension for a U.S. Department of Homeland Security ("DHS")-approved reason, the drivers' licenses of that state will not be an acceptable form of personal identification for "official purposes." For example, because the State of Oklahoma has refused to comply with REAL ID, an Oklahoma resident will not be able to use his or her drivers' license as personal identification to board a plane or enter a federal building or federal park. Such a citizen would have to use a passport or other REAL ID compliant form of identification. The term "official purposes" has been left intentionally vague, leaving great discretion to DHS to add more activities in the future as it deems necessary and prudent. Other federally regulated activities include, but are not limited to, gun purchases, voting, and certain banking transactions.

Among many of its laudable goals, REAL ID sets standards for tamper-proof identification cards, requires verification of citizenship for card issuance, and calls for background checks and screening of DMV employees. REAL ID sets security standards for state DMV and card manufacture facilities. "Breeder documents" (*e.g.*, birth certificates) must be presented and scanned into permanent electronic storage. While authentication of breeder documents within the United States is a legitimate expectation, the incorporation of electronic copies of such documents into a database system accessible by foreign officials, not governed by U.S. privacy law, is cause for concern. Moreover, that the personal information and biometric data of common citizens will be incorporated into this system is disconcerting. Naïve reliance on existing data protection and privacy laws seems misplaced, especially since such laws appear outdated and irrelevant in light of modern technological advances and global cooperation.

Among some of its more controversial goals, REAL ID relies heavily on the wholesale collection and use of biometric identifiers, such as the high-resolution digital facial photograph, fingerprint, and signature recognition. A high enough resolution photograph also enables the use of iris-scanning technology. DNA make-up and voice recognition are other types of biometric identification under development. The digital facial photographs required under REAL ID meet technology requirements that will soon allow individual faces to be identified by live, real-time video "security" cameras. While collection and use of such data domestically poses issues meriting vigorous debate, the impact of the interoperability of data and databases worldwide combined with international trends in data collection must be discussed openly and considered carefully by citizens and elected leaders alike.

Currently, at least thirty-five states have expressed varying degrees of concern over REAL ID and have bills in various stages of the legislative process. Many states, such as Oklahoma, have already rejected REAL ID outright. It appears that the swell of opposition is growing and gaining momentum.

II. REAL ID IN THE CONTEXT OF VARIOUS FEDERAL INITIATIVES

Our research revealed that REAL ID is but one of several federal initiatives involving data collection, storage, and sharing. Many DHS and other federal initiatives are based on electronic and biometric data collection, storage, use, and sharing, and are in various stages of implementation. Such initiatives include:

- Registered Traveler Program
- Secure Flight Program
- E-Passport
- US-VISIT
- Western Hemisphere Travel Initiative ("WHTI")
- Transportation Workers Identification Credential ("TWIC")
- Security and Prosperity Partnership of North America ("SPP")
- US-EU Passenger Name Record ("PNR") Agreement
- Federal Election Reform
- Electronic Health Records ("EHR")

These programs and agreements, like REAL ID, are built on international trends in personal data collection, storage, use and sharing (to use the UN's term—"civil registration"). They reflect the *internationally* implemented efforts to replace "hard" borders with transparent "smart" borders, creating "Global Security Envelopes" to facilitate changing demands in the transportation of goods and people. "Interoperable" biometrically tagged "smart" cards and expansive inter-connected databases are the backbone of the proposed systems of the future.

While governmental systems of expansive data collection and sharing certainly did not begin with, and are not unique to, REAL ID, the application of such systems to citizen drivers' licenses and identification cards does represent an unprecedented and much broader initiative. Moreover, the extent of international involvement in the proposed REAL ID database system implicates national sovereignty issues in addition to the concerns expressed by many Americans that their personal information and biometric data will be made available outside the United States, without the citizen's knowledge or consent.

REAL ID proponents assert that the REAL ID initiative is a result of the 2004 9/11 Commission report. However, at least as early as 1996, various forms of a national ID card system had been introduced into the legislative process—REAL ID is the first to come close to actual implementation. Moreover, REAL ID is the realization of the international community's objectives which long preceded the attacks of 9/11.

III. INTERNATIONAL ISSUES RAISED BY REAL ID

Years before the attacks of 9/11, the American Association of Motor Vehicle Administrators ("AAMVA") sought a unified North American drivers' license and record database (the Driver License Agreement, "DLA"). AAMVA views REAL ID as a key step towards realizing its goal. REAL ID incorporates a linking of state electronic DMV databases which will collect, store, use, and share biometric data, namely the high-resolution digital portrait. It appears that AAMVA will operate this database linking system. AAMVA is an international organization; hence, it represents interests beyond those of the United States, or any particular State. It appears that the issue of REAL ID has forced many state legislatures to reconsider the amount of discretion given to their DMV's, due to the level of dependence on AAMVA most DMV's have developed.

As you may be aware, REAL ID also complies with certain technical requirements set by the United Nation's International Civil Aviation Organization ("ICAO"). DHS and ICAO are also working together, along with numerous agencies in other nations, to implement data collection and sharing programs related to airline passengers (*e.g.*, Registered Traveler Program, Secure Flight). It appears that the UN is heavily involved in the growing international trends of personal data collection, storage, and use. Moreover, it appears that the REAL ID system is being engineered to be interoperable worldwide. The concerns raised by REAL ID's semblance to clear international trends, to our knowledge, have not been adequately addressed. DHS has clearly indicated its intentions to share U.S. citizens' biometric and other data with other nations, international organizations, and security corporations, and indeed has already implemented such programs. While the collection and sharing of data pertaining to known or suspected international terrorists is a practical and constitutionally sound mechanism for national defense, it appears REAL ID and its related initiatives expand this mechanism to collect, organize, and dispose of the personal and biometric data of common, law-abiding citizens.

REAL ID should not be analyzed in isolation from other related initiatives here in the U.S. Instead, it is important to also consider related developments and initiatives around the globe. For example, the United Kingdom, Egypt, Iraq, and China either already have or are moving to implement a modern "smart" national ID card, and each collects religious affiliation data in its census. Nations with national ID cards often collect religious data from citizens, and as in Egypt, this religious data ends up on the card, directly affecting the holder's legal status in the country. Nations with ID cards are increasingly conditioning receipt of Government services, entitlements, or privileges on a satisfactory status. Very often, international trends in religious data collection and national ID cards are connected to disturbing discrimination and even violence against religious or ethnic minorities. Regardless of such abuses, the UN actively promotes the collection of as much data as possible by governments, specifically recommending the collection of religious information. For example, it is reported that ID cards in China contain electronic data such as a citizen's high-resolution digital photograph, *religion*, ethnicity, police and health records, and reproductive history. Much of this data will be contained within RFID chips inside the cards. Surveillance cameras installed along streets in certain parts of China will automatically identify passing citizens by the stored digital photograph. Closer to home, U.S. neighbors Canada and Mexico collect religious affiliation data in their national censuses. Both

neighbors will be connected to the U.S. through AAMVA's stated "one-driver, one-record" REAL ID jurisdictional scheme. Further, they are increasingly tied to U.S. interests as the North America Free Trade Agreement ("NAFTA"), Security and Prosperity Partnership ("SPP"), and smart-borders of the future are implemented.

IV. BALANCING THE LEGITIMATE GOVERNMENTAL INTERESTS IN NATIONAL SECURITY WITH INDIVIDUAL LIBERTIES

Islamic extremism is changing the world, as well as the American way of life. Many of the changes were inevitable, even necessary, in a post-9/11 world dominated by non-traditional warfare against shadowy international terrorist organizations. The United States Constitution permits that, as various interests are balanced in times of war, individual liberty may sometimes necessarily yield to the Government's legitimate, and, indeed, primary interests in ensuring national security and preserving national sovereignty. In western liberal democratic systems, however, this understanding does not require that all governmental decisions that effect the balance between national security, sovereignty, and individual liberty be made outside of the public's knowledge or against the public will. Indeed, the Constitution also protects the citizenry's right and duty to stay informed and to influence its Government.

Moreover, United States sovereignty should not be casually exchanged for perceived gains in international security or international trade. On the contrary, a vibrant national sovereignty is the surest and most legitimate mechanism for ensuring security in the international realm. Although a degree of cooperation is necessary in an increasingly interconnected world, it would be imprudent to entrust U.S. security interests to the diverse and competing interests represented within the international community. Besides the privacy implications of sharing citizens' data abroad, a careless approach to international cooperation could well lead to an attenuation or even redistribution of power and technological advantage at the expense of the long term national interests of the United States. Collecting and electronically linking U.S. citizens' data raises concerns, not just of privacy but also of further federal governmental expansion and centralization. Sharing such data with international entities and foreign nations significantly raises the stakes. While many post-9/11 strategy changes were needed and long overdue, most changes focused on targeting the communications, financial transactions, and travel, of the suspected terrorists. New trends appear to focus more broadly, directly impacting common citizens. The American people ought to be aware of the implications and engage the debate.

Furthermore, while the addition of biometric data to an individual's electronic file may add a layer of protection against certain types of common fraud, the inclusion of such data also greatly heightens its value for fraudulent use. That these electronic databases or networks are subject to security breaches is reported almost weekly. Recent examples include: the UK's loss of discs containing tax, benefits, and related personal data records for half of its population; the infiltration of the Pentagon network by the Chinese military – accomplished in as little as a few months; and the breach of the USAJOBS executive branch database subcontracted to the private sector job source, Monster. It is undisputed that there is no perfect or foolproof "system," but

REAL ID proponents insist that risk allocations are necessary. This may or may not be the case, but our initial concern is the apparent lack of general public knowledge on an issue that will significantly impact the lives of law-abiding citizens. Regardless of Governmental intent, it appears that the REAL ID data collection and database linking system would set in place a system which allows the movement and activities of all citizens to be tracked, as is done in China.

Many of REAL ID's objectives are legitimate, even necessary; however, some pose concerns and merit in-depth consideration. REAL ID was passed with little to no debate or public involvement, yet it significantly impacts all law-abiding citizens. Many DMV activities, such as standardization and interoperability compacts, take place largely outside of the legislative process, and outside of public view. Legislative oversight and vigorous debate is needed in such a comprehensive issue. REAL ID's overwhelming passage in the U.S. Senate and House contrasts starkly with its growing opposition among states. State legislators, along with state citizens, should communicate with their U.S. congressional delegations regarding each state's policy position on these issues. It is an *absolute necessity* that all data included in such a system be secured. As of yet, there are grave doubts that the required level of security has been, or can ever be, achieved.

Again, we appreciate that you brought these issues to the ACLJ's attention. The ACLJ will carefully monitor the situation. We value your perspective as legislators of the State of Oklahoma, and we are grateful for the opportunity to be of assistance. If you have further questions or concerns, please do not hesitate to contact us.

Sincerely,

Robert W. Ash
Senior Litigation Counsel for
National Security Law

cc: Representative Mike Reynolds
Representative Jason Murphey
Representative Sally Kern
Senator Randy Brogden

About AAMVA

Strategic Plan | General Information | Office Hours and Holiday Schedule

The American Association of Motor Vehicle Administrators (AAMVA) is a tax-exempt, nonprofit organization developing model programs in motor vehicle administration, law enforcement and highway safety. The association also serves as an information clearinghouse in these areas, and acts as the international spokesman for these interests.

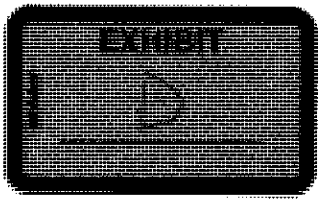
Founded in 1933, AAMVA represents the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws. AAMVA's programs encourage uniformity and reciprocity among the states and provinces. The association also serves as a liaison with other levels of government and the private sector. Its development and research activities provide guidelines for more effective public service. AAMVA's membership includes associations, organizations and businesses that share an interest in the association's goals.

AAMVA has four regions incorporated under its umbrella.

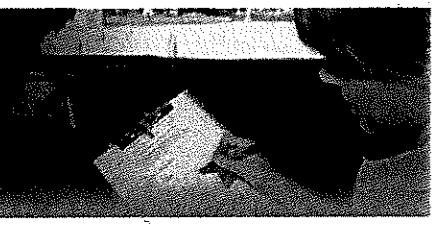
Related Content

AAMVA Policy Positions
AAMVA Bylaws
Contact Us
Staff Listing
Biographies & Photos
AAMVA Lexicon (glossary of terms)
Commonly Used Acronyms
Report Legal/Ethical Violations

AAMVA celebrates its 80th anniversary!



Driver Licensing & Identification



Licensing and Identification | Committees and Working Groups | Certification Programs | Best Practices

Key among AAMVA's goals is improving highway safety and identification security by promoting uniform standards for all areas related to driver licensing. AAMVA is committed to improving driver safety and to the "one driver, one record" driver's license concept. Learn more about:

- DL/ID Standards
- Identification Security
- At-risk Driver Programs
- Motorcycle Licensing
- Commercial Driver Licensing
- International Licensing
- Driver License Compacts
- Auto Insurance/Financial Responsibility

Related Content

Driver Standing Committee

Driver Licensing Systems

- CDLIS
- CSTIMS
- DVD
- EDL
- FEWS
- PDPS
- SR 22/26
- SSR

Verification Systems

- DIA
- EVVER
- HAVV
- RIDE
- SSOLV
- VLS

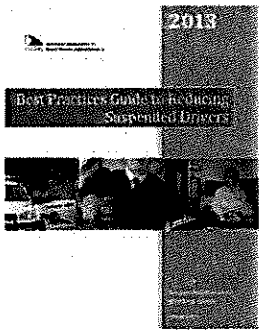
2012 DL/ID Card Design Standard

Updates to the DL/ID Card Design Standard (CDS) include:

- veteran indicator element (optional human and machine-readable)
- courtesy verification program section
- note regarding overlap of zones
- More!

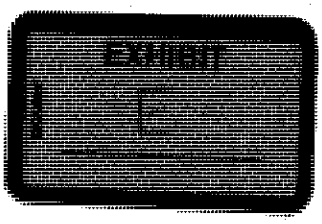
February 2013

Best Practice Guide to Reducing Suspended Drivers



AAMVA Working Group Releases "Best Practice Guide to Reducing Suspended Drivers"

The suspension of driving privileges has been used for decades to address poor driving behavior. However, what was originally intended as a sanction to address poor driving behavior is now used as a mechanism to gain compliance with non-highway safety, or social non-conformance, reasons. Eliminating suspensions for non-highway safety violations will significantly reduce the burden on DMVs, law enforcement, the courts and society. AAMVA's Suspended/Revoked Working Group recommends that legislatures repeal state laws requiring the suspension of driving privileges for non-highway safety related violations. Download the document today to learn more.



Watch a video for a quick snapshot of the issue.

DL/ID Standards

General Information | Documentation | Courtesy Verification Program | Card Design Standard Committee

The DL/ID Card Design Standard (CDS) was developed by the Card Design Standard committee made up of jurisdictional and federal government members. The CDS provides for the design of driver licenses (DL) and identification (ID) cards and its intent is to improve the security of the DL/ID cards and the level of interoperability among cards issued by all North American jurisdictions.

2012 DL/ID Card Design Standard Released!

AAMVA is happy to announce the release of the 2012 AAMVA DL/ID Card Design Standard (CDS). The 2012 CDS supersedes the 2011 AAMVA DL/ID Card Design Standard. AAMVA strongly recommends that jurisdictions beginning new card design and production efforts base their work on the 2012 standard. The 2011 AAMVA DL/ID Card Design Standard, along with previous versions, will continue to be available since jurisdictions have cards in production that are based upon those specifications.

The following is a summary of changes between the 2012 CDS and the previous version (2011).

- Courtesy Verification Program section added
- Normative References added/updated...
  - European Commission Directive 2006/126/EC of 20 December 2006 O.J. EC No. L 403/18
  - ISO 1073-2:1976: Alphanumeric character sets for optical recognition -- Part 2: Character set OCR-B -- Shapes and dimensions of the printed image
  - ISO 8601:2004: Data elements and interchange formats -- Information interchange -- Representation of dates and times
  - EPC Tag Data Standard (Available from www.gs1.org/gsmp/kc/epcglobal/tds/)
  - EPC Generation 2 Air Interface Specification (Available from http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/)
- Veteran Indicator element has been added (optional human & machine-readable)
- Note re overlap of zones has been added
- Re-write on Annex H. stripping out most of the original narrative and areas that went beyond the scope of the standard

Download the updated CDS

Other Resources

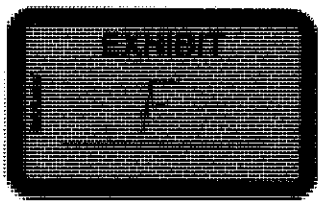
International Licensing and Standards

Technology Standards

Links to Other Standards Resources

Statement Regarding DL/ID Samples

AAMVA does not provide sample DL/ID documents / specimens / exemplars from our principal membership - for questions related to such requests please contact the issuing authorities directly.



Card Design Standards Committee

Mission | Guiding Principles and Objectives | Committee Roster

Cindy Gerber, South Dakota (Chair)

Scott Vien, Delaware (Vice Chair)

Pat McCormack, Minnesota (Board Liaison)

Kim Lambert, Ontario (Region I)

Barbara Webb, North Cerolina (Region II)

Stephen Leak, Indiana (Region III)

Ted Ockenden, British Columbia (Region IV)

Capt. Leonard Casper, New York (Law Enforcement Liaison)

Robert Rousse, Quebec (CCMTA)

DHS (Advisory)

Loffie Jordaan (AAMVA)

Geoff Slagle (AAMVA)

Related Content

DL/ID Card Design Standard

Driver Standing Committee

Contact: Geoff Slagle

Biometrics

Biometrics Background
The Technologies
Common Applications
FAQs
Glossary

Become a Member

Biometrics Background

The Origins of Identity

From earliest times, man has sought means to determine who was and who was not a member of a particular group; or who was to be accorded specific rights and privileges as a result of his relationship with or status within a group.

As civilization moved beyond a point that everyone in a community knew everyone else, names, (frequently reflecting paternal lineage or one's role in a community - John's son, or John Smith - are examples) were adopted. But when the number of "John Smiths" increased to a point where name alone could no longer clearly discriminate, or when John Smith ventured farther out in a world where he knew no one, and nobody knew him, other identity conventions were needed.

Identity and the ability to authenticate it is a critical component of collective security in a world where ideas, information and capital move at the push of a button, and where anyone can get anywhere in a matter of hours. Today, personal identity and the ability to prove it can influence where one lives, where one can travel, whether one can be trusted as a partner in commerce, as well as one's ability to access information or resources.

As we face new social, political, and economic challenges in the 21st century, it is fitting that underpinnings of collective security rest on biometrics, technologies that reflect the uniqueness of the men, women and children living in societies we strive to create and improve upon.

These biometric technologies can make our world safer and reduce risk. Biometrics can also introduce convenience and labor-saving to our lives. Biometrics can help re-engineer business processes, helping private enterprise to thrive and reducing burdens on strained public sector infrastructures so they can be more productive for constituents. And biometrics can do all this, not at the expense of privacy, but rather by assuring privacy's very survival.

Biometrics - Physical & Behaviorally-Based Identity Authantication

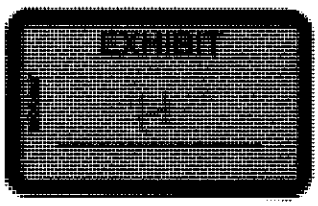
Instead of basing identity authentication on what someone possesses or what someone knows, biometric identification is based on what one is, or how one behaves, This approach to identification is made possible by technology developments that enable precise measurement coupled with computational power that allows measurements to be transformed into mathematical representations that can be rapidly compared.

- **The Unique Physical Attribute**
  Fingerprints on cards, and lifted from the scene of a crime have been used for more than one hundred years as proof of individual identificetion for forensic and law enforcement purposes. Once time-consumingly collected as inked sets on cards, they are now routinely collected by electronic or optical sensors that turn patterns once only defined as whorls and arches into mathematical representations called biometric templates. Other physical attributes that can be measured and converted into mathematical representations include: faces, fingerprints, hands, iris patterns, retinal patterns, vein patterns, voice patterns, and DNA. Exploratory work has been done to establish whether physical characteristics such as earlobes and body odor can be effectively measured, mathematically represented, and rapidly compared for use in electronic identity authentication.
- **The Unique Behavioral Attribute**
  Measurable mathematical values that can be quickly compared to establish an association with a specific person can be assigned to not only physical traits, but also to behavioral traits. Templates reflecting individual characteristics exhibited in signing one's name - the speed, angle of the pen and pressure exerted, as well as the physical appearance of the signature itself-are used in signature dynamics. Unique patterns that emerge in studying individual self-expression are not limited to handwriting. The way one interacts with a keyboard can also be studied, measured, and committed to mathematical representation in keystroke dynamics. And behavioral attributes aren't relegated to things related to up-close personal expression. The unique ways

Our Mission

To advance adoption of responsible use of identification technologies for managing human identity

Follow Us On



in which a person moves when walking can be, and is observed, measured and expressed mathematically in a technique known as gait recognition-one of the biometric technologies most suited to personal identification at a distance.

Benefits of Biometrics Compared to Traditional Identity Conventions

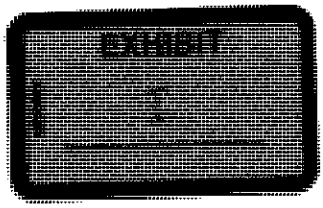
One approach to establishing the identity of an individual was based on tokens. A token was, and remains, something a person possesses and uses to assert a claim to identity. The passport that once took the form of a letter from the king asking all who saw it to guarantee safe passage to the bearer– is still one of many tokens, things one possesses, routinely used for personal identification.

Sometimes ascertaining identity required an individual have some specific special knowledge, known only by a person with bonafides. Whether a single word, a phrase, an alphanumeric combination entered on a keyboard, or a response to a challenge - "last four digits of your social," "mother's maiden name," or "shortstop for the Dodgers," etc. - what one knows remains a common practice in deciding whether an individual's claim of identity should stand - or not.

While widely used to this day, tokens and special knowledge are by themselves no longer sufficient to authenticate identity. If in possession of the token or facsimile, or having by accident or design acquired the required piece of knowledge, it is relatively easy to represent that one is someone, whom in fact, they are not.

Face

Our faces make lasting impressions. Despite the growing popularity of cosmetic surgery, research has shown that the face we are born with remains identifiable throughout our lives. The relationships between the parts of the face, its curves and contours, remain relatively stable from childhood onward. Facial recognition techniques use this stability as their point of departure. Facial recognition technologies utilize digital photographs to create mathematical descriptions of individual faces and then compare them against those stored in a database. Facial recognition requires a large image capture device and clear lighting conditions and is therefore most suitable to authenticate identity at fixed locations, such as facility access points. Facial recognition data are also being encoded via mobile technologies, such as the new generation of biometric passports



Mission

About Us

Mission
Why Join IBIA?
Current Members
Membership Classification
Become a Member
Board of Directors
Management Group
Working Groups
Privacy Principles
Ethics Statement
Contact Us

Become a Member

The **International Biometrics & Identification Association** (IBIA) is a trade association founded in September 1998 in Washington, DC that promotes the effective and appropriate use of technology to determine identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.

Recognizing the vital role identity plays in a globally connected world, IBIA brings stakeholders into a single organization that provides a

- forum for exchanging information and ideas;
- clearinghouse for resolving issues and establishing policy;
- voice for policy advocacy and education;
- connection to complementary organizations and standards bodies.

Our key focus is on the use of technology in determining identity. Biometrics, which is one of the technologies playing an increasingly important role in identity management, has reached our everyday lives. It is commonly embedded within solutions that protect national borders and ports; enhance programs like driver's licenses and social benefits registrations; secure facilities like daycare centers, banks, health clubs, and schools; prevent identity theft; secure data and transactions for financial and health care institutions; and protect personal data in laptops and mobile phones.

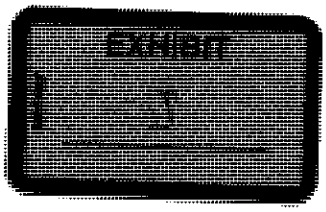
Our Mission

- Promote using technology effectively and appropriately to determine personal identity and enhance security, privacy, productivity, and convenience for individuals, organizations, and governments.
- Advocate for and actively engage in developing public policy on personal identification issues;
- Collaborate with consumers, providers, associations, and entrepreneurs to help them use biometrics to achieve effective security and business solutions;
- Provide a forum to exchange information and ideas, bring visibility to the latest advanced biometric research, resolve issues, and establish policy positions;
- Provide information on important national and international technology and policy developments;
- Participate in relevant national and international technology standards bodies.

Our Mission

To advance adoption of responsible use of identification technologies for managing human identity

Follow Us On



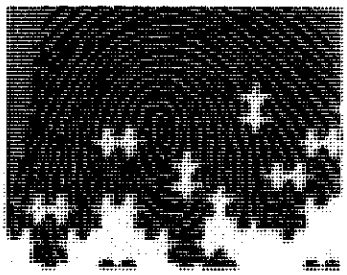
National DEFENSE
NDIA
NDIA's Business and Technology Magazine

Biometrics

Defense Department Under Pressure to Share Biometric Data

January 2009

By Stew Magnuson



TAMPA, Fla. — Within minutes of knocking down the door of a suspected bomb maker in Iraq, U.S. troops can fingerprint everyone they find inside, send the scans across a satellite link, and find out if the subjects are suspected terrorists.

Military police in the Middle East who are manning checkpoints or sifting through job applicants for local hires can use the same technology.

Biometrics — the science of identifying a person through his unique body measurements such as fingerprints, iris scans, voice prints or even DNA — has come into its own. Operations in urban areas against enemies who don't wear uniforms make identifying friends and foes more important than ever.

Technologies that allow investigators to identify suspected terrorists have been sped into the field, but these efforts are not being well coordinated, and that can lead to critical information gaps, and so-called stovepipes, the common term for information and communication systems that cannot link to each other, experts at the Biometrics Consortium conference said.

There are signs that progress is being made, government officials said. A presidential directive that was signed last year will help federal agencies sort out who does what in terms of identity management. The Naval Post Graduate School announced that it will begin a master's level program in identity management. And Customs and Border Protection is now collecting 10 fingerprints from visitors arriving from foreign countries.

But is all this enough?

"We are still in the throes of a paradigm shift," said Donald Loren, deputy assistant secretary of defense for homeland security integration.

When he walks into the Pentagon, he still flashes an ID badge with a mug shot.

"That's identification. That's not identity management," he said.

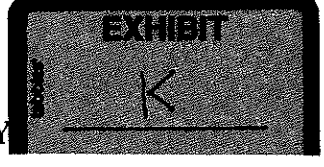
Biometrics is the science behind the larger issue of "identity management." Collecting a fingerprint is fine, but how should the government store, secure and share — when necessary — the biometric data it collects?

Along with the military services, entities such as the State Department, the Coast Guard, Customs and Border Protection, the Department of Justice and its law enforcement arms such as the FBI — are involved in collecting biometric data.

"The Defense Department is still in the discovery phase of interagency, international and civil support activities" when it comes to biometrics and identity management, said Loren.
"We have to continue to work out the problems," he added.

The release of National Security Presidential Directive 59 outlined the steps the federal government must take to coordinate all these efforts.

The Defense Department has also set up several working groups and committees to tackle the problem. The National Science and Technology Council subcommittee on biometrics and identity management and the Defense Department's biometrics readiness group are among them.



"We don't have a single belly button for biometrics in the Defense Department," said Tom Dee, who is the point man for the field in the Director of Defense Research and Engineering office. He is charged with keeping an eye on all these programs and ensuring there is a "unity of effort."

The deputy secretary of defense signed a directive in February defining roles and responsibilities in the Defense Department. The Army remains the executive agent for biometrics, even though that doesn't mean it is buying systems for the Navy or other services, Dee said.

Two recent Government Accountability Office reports called into question the effectiveness of these Defense Department efforts.

"While [the Defense Department] has stated some general goals for biometrics, such as providing recognized leadership and comprehensive planning policy, it has not articulated specific program objectives, the steps needed to achieve those objectives and the priorities, milestones, and performance measures needed to gauge results," said the report titled "DoD Needs to Establish Clear Goals and Objectives, Guidance and a Designated Budget to Manage its Biometrics Activities."

As the title suggests, the Defense Department needs a designated budget for biometrics — a "program of record" — that links resources to specific objectives and provides a consolidated view of the resources devoted to such activities, the report said.

So far, the Pentagon is relying on initiative-by-initiative requests for supplemental funding, the report said.

A second report, "DoD Can Establish More Guidance for Biometric Collection and Explore Broader Data Sharing," gave a clear example of how the lack of a cohesive strategy for the use of biometrics can undermine military operations.

U.S. forces encountering hostile individuals in Iraq and Afghanistan collect different biometric data. It's up to the battlefield commanders to decide whether they want to collect fingerprints, iris scans or both. "Allowing for this flexibility results in the collection of different data that are not necessarily comparable to each other," the October report said.

"Broader national security implications can arise, such as military personnel's inability to identify someone who has harmed or attempted to harm U.S. or coalition forces," the report added.

Despite a memo declaring the Defense Department would share all its unclassified biometric information in the spirit of interagency cooperation in the war on terrorism, the Department of Homeland Security complains that it is not receiving regular updates of data it could use, the report said.

Al Miller, a consultant to the office of homeland defense and America's security affairs, said at the conference that the FBI spent one year trying to track down who in the Defense Department could sign off on a biometrics information sharing agreement.

In written responses to the September GAO report, the Defense Department said it is moving toward making its biometrics efforts programs of record, although not all technologies will neatly fit into one line in the budget. It expects this to happen in the fiscal year 2010 budget request.

As for a lack of data sharing, the Defense Department maintains its own watch list, and said it is sending all the information in it to DHS when the law allows.

Meanwhile, the fight to rid Iraq of roadside bombs is showing how effective biometrics can be in an insurgency, said Konrad Trautman, director of intelligence at Special Operations Command.

Biometric tools, when used on raids on suspected bomb makers' safe houses, have helped to kill or capture individuals who are involved in the construction of improvised explosive devices at the average rate of two per day for the last two years.

"How many bombs would have been made by those individuals if they were still on the battlefield?" he asked.

The goal is to rapidly exploit the evidence found on a raid site including everything the suspects have touched. There might be five men who claim to be innocent bystanders on the scene. But one might be the operation's paymaster. All that has to be sorted out as soon as possible, Trautman said.

Collector ID kits are used to gather fingerprints and mugshots. Those records are sent via a small satellite dish to three databases at the Defense Department's biometrics fusion center, the Army's national ground intelligence center, and the FBI's automated fingerprint identification system.

The Defense Department has about 2.2 million files, and the FBI has another 58 million.

Through September, special operations forces have sent 28,000 submissions, with 8,000 matches coming back. And 1,722 of them positively identified the subject as part of an IED cell.

The goal is to receive a response back within 15 minutes. In fact, the usual response time is much quicker — about four

and a half minutes, Trautman said.

Other tools, such as link analysis software, can begin to build pictures of a bomb-making network. If intelligence officers can establish a link to another suspect, and they know where he lives, the goal is to launch a second raid within an hour, Trautman said.

This all works great in Iraq where U.S. forces have a free hand, and there isn't an American Civil Liberties Union lawyer in sight. They can collect biometric data — even their DNA in some cases — from about anyone they encounter from a known or suspected terrorist, a job applicant or a petty thief.
But when operating in other nations, U.S. forces cannot count on having this kind of freedom.

There are no international treaties covering such matters, said Dee.

There are "shady areas" when it comes to collecting biometrics, he admitted. It will depend mostly on bilateral agreements. "It would be up to the host nation for what we're permitted or not permitted to do," he said.

Two advocacy groups, Human Rights Watch and Privacy International, wrote a joint letter to Defense Secretary Robert Gates in July 2007 questioning the collection of biometric data from ordinary Iraqi citizens, who aren't suspected of breaking any laws.

"We recognize the strategic military importance of identifying threats to American military personnel," the letter said. "However, these tactics also strip away a substantial privacy measure for Iraqi citizens in the midst of a conflict that flows from deep religious and ethnic division."

The letter questioned what would happen if the data were turned over to Iraqi authorities and then later misused.

"The massive aggregation of secret files on Iraqis, linked to permanent biometric identifiers, creates an unprecedented human rights risk that could easily be exploited by a future government," the letter said.

William Gravell, special adviser to the secretary of the Navy for identity management, and several other Defense Department officials, acknowledged that if privacy is not protected, then public acceptance for biometrics will evaporate. It will become one of those technologies that works well, but is not acceptable to use.
"Strong identity management does not necessarily mean weak privacy," he said.

Capt. John Boyd, the Navy's program manager for identity management capability, said the Navy during the last two years has collected only a few hundred mugshots and fingerprints.
The rules for what the Navy can do when boarding a foreign vessel "are totally different from Iraq or Afghanistan," he said.

Trautman said that having the right policies, techniques and procedures in place for partner nations will become vital.

"The policy allows us to lash that together, not just for the domestic intelligence concerns but international policy as well or bi-national policy," he said.

Miller said the United States has bi-lateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement.

He expressed some concern that the momentum for identity management within the federal government, and the efforts to sign these agreements, will falter with the change in administration in 2009.

"Today's policies are stressing the negative — who are the bad guys," Miller added.

"We have to look at some goodness at what we are doing — protecting those on bases and their families with biometrics."

Reader Comments

Re: Defense Department Under Pressure to Share Biometric Data

COMMENT
Several Policies, Procedures and Processes need to be implemented before this dream can come true:
• An over all governance must be put in place, one that is empowered to walk the walk
• All US security, armed services and undercover agencies wide acceptance (no special cases) NO special cases
• Any person entering US buildings, installations, US boarders must be able to have there identity validated from all watch databases, NO acceptations, leave visitors and US citizens that have NO business entering these US assets alone.
• A technology that is developed and put in place that will conform all existing fingerprints and newly captured fingerprints, regardless of the capture and stored algorithm (do not re-create the wheel, use what we have) with availability to the right to know incorporated
• Multiple redundancy for data recovery and protection,
• Secured FP transfer protected by unbreakable technologies, NANO/Photon technology plus long encrypted algorithms/PKI

Paul Zaren on 01/06/2009 at 13:20

Submit Your Reader's Comment Below

***Name**

***eMail**

The content of this field is kept private and will not be shown publicly.

***Comments**

Please enter the text displayed in the image.
The picture contains 6 characters.

***Characters**

***Legal Notice**

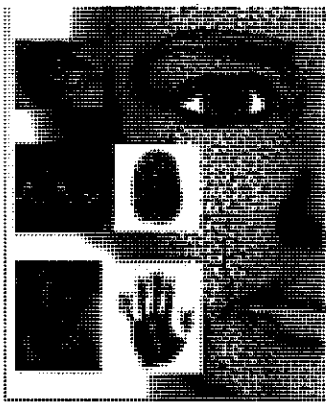
NDIA is not responsible for screening, policing, editing, or monitoring your or another user's postings and encourages all of its users to use reasonable discretion and caution in evaluating or reviewing any posting. Moreover, and except as provided below with respect to NDIA's right and ability to delete or remove a posting (or any part thereof), NDIA does not endorse, oppose, or edit any opinion or information provided by you or another user and does not make any representation with respect to, nor does it endorse the accuracy, completeness, timeliness, or reliability of any advice, opinion, statement, or other material displayed, uploaded, or distributed by you or any other user. Nevertheless, NDIA reserves the right to delete or take other action with respect to postings (or parts thereof) that NDIA believes in good faith violate

☐ I have read the Legal Notice.

Submit

Biometrics.gov

Welcome



Biometrics.gov is the central source of information on biometrics-related activities of the Federal government. This site and its sister site, www.biometrics.org, provide a repository of biometrics-related public information and opportunities for discussion. These websites, working together, were developed to encourage greater collaboration and sharing of information on biometric activities among government departments and agencies; commercial entities; state, regional, and international organizations; and the general public.

Biometrics.gov provides basic information and links to specific biometric activities in the Federal government. The site includes four main "rooms":

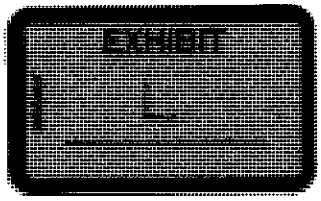
- Biometrics Reference. This room provides general information about biometric technologies, government programs and privacy planning
- Presidential Directives. This room provides text of Presidential Directives that touch on biometrics or federal biometric activities
- NSTC Subcommittee on Biometrics and Identity Management Room. This room provides information on the National Science & Technology Council's Subcommittee on Biometrics and Identity Management. The NSTC, a Cabinet-level Council, is the principal means within the executive branch to coordinate science and technology policy across the diverse entities that make up the Federal research and development enterprise.
- Standards. This room provides information on federal biometric standards policy, and a registry of recommended standards.

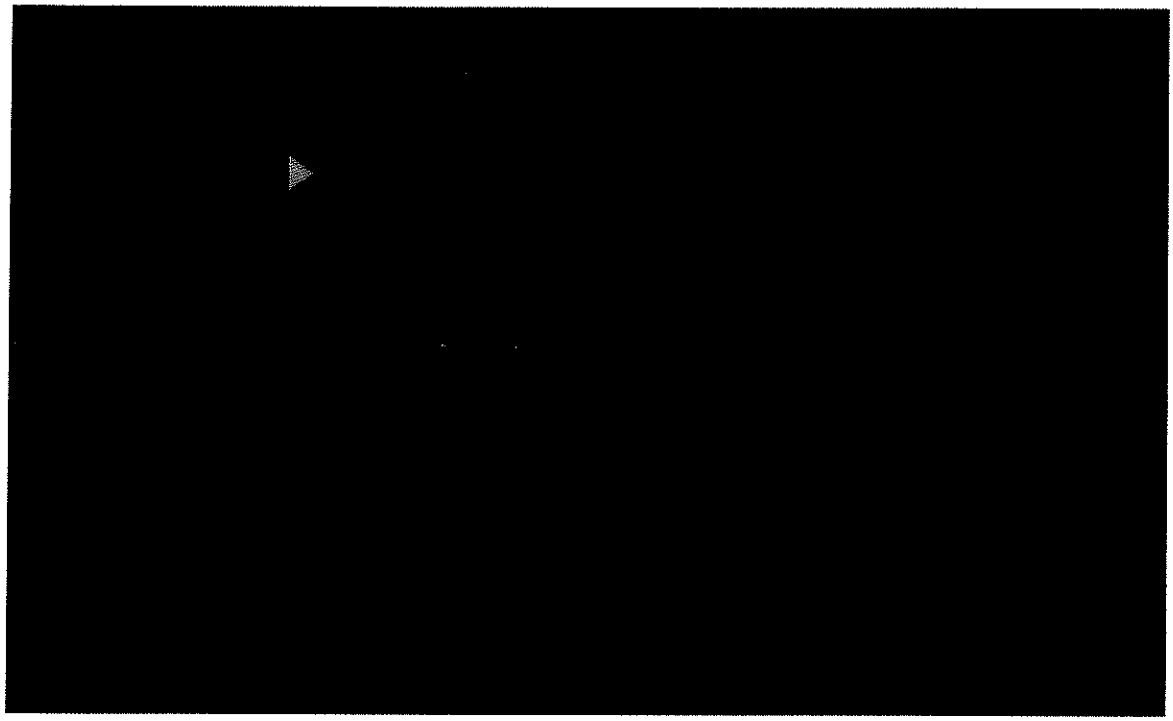
The National Biometrics Challenge 2011 NEW

During the last five years, evolving mission needs, coupled with advances in technology, have necessitated a new look at biometric priorities. This 2011 update to *The National Biometrics Challenge* examines the many advances made as government, academia, and the private sector have collaboratively responded to the priorities identified in 2006. It also delineates some of the challenges that, five years later, have yet to be fully addressed — and offers some new goals that might previously have seemed beyond reasonable hope of being attained but that today appear achievable in light of new technologies. [Download]

BCC 2011 Opening Video: NEW

Since the events on September 11, 2001, the biometric community has made vast technological improvements in protecting the United States and its borders. This video will provide an overview of the advancements in biometric technology across the Federal Government since 9/11. Hi-Res Video (51M) located below, please click the play button. To view the low-res (13M) version click here.





NSPD-59 / HSPD-24

The White House
President George W. Bush

For Immediate Release
Office of the Press Secretary
June 5, 2008

National Security Presidential Directive and Homeland Security Presidential Directive

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE/NSPD -- 59
HOMELAND SECURITY PRESIDENTIAL DIRECTIVE/HSPD -- 24

SUBJECT: Biometrics for Identification and Screening to Enhance National Security

Purpose

This directive establishes a framework to ensure that Federal executive departments and agencies (agencies) use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting their information privacy and other legal rights under United States law.

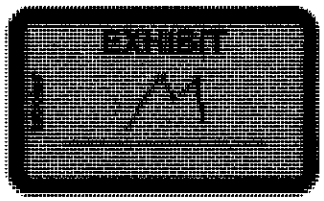
Scope

(1) The executive branch has developed an integrated screening capability to protect the Nation against "known and suspected terrorists" (KSTs). The executive branch shall build upon this success, in accordance with this directive, by enhancing its capability to collect, store, use, analyze, and share biometrics to identify and screen KSTs and other persons who may pose a threat to national security.

(2) Existing law determines under what circumstances an individual's biometric and biographic information can be collected. This directive requires agencies to use, in a more coordinated and efficient manner, all biometric information associated with persons who may pose a threat to national security, consistent with applicable law, including those laws relating to privacy and confidentiality of personal data.

(3) This directive provides a Federal framework for applying existing and emerging biometric technologies to the collection, storage, use, analysis, and sharing of data in identification and screening processes employed by agencies to enhance national security, consistent with applicable law, including information privacy and other legal rights under United States law.

(4) The executive branch recognizes the need for a layered approach to identification and screening of individuals, as no single mechanism is sufficient. For example, while existing name-based screening procedures are beneficial, application of biometric technologies, where appropriate, improve the executive branch's ability to identify and screen for persons who may pose a national security threat. To be most effective, national security identification and screening systems will require timely access to the most accurate and most complete biometric, biographic, and related data that are, or can be, made available throughout the executive branch.



(5) This directive does not impose requirements on State, local, or tribal authorities or on the private sector. It does not provide new authority to agencies for collection, retention, or dissemination of information or for identification and screening activities.

Definitions

(6) In this directive:

(a) "Biometrics" refers to the measurable biological (anatomical and physiological) and behavioral characteristics that can be used for automated recognition; examples include fingerprint, face, and iris recognition; and

(b) "Interoperability" refers to the ability of two or more systems or components to exchange information and to use the information that has been exchanged.

Background

(7) The ability to positively identify those individuals who may do harm to Americans and the Nation is crucial to protecting the Nation. Since September 11, 2001, agencies have made considerable progress in securing the Nation through the integration, maintenance, and sharing of information used to identify persons who may pose a threat to national security.

(8) Many agencies already collect biographic and biometric information in their identification and screening processes. With improvements in biometric technologies, and in light of its demonstrated value as a tool to protect national security, it is important to ensure agencies use compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric information.

(9) Building upon existing investments in fingerprint recognition and other biometric modalities, agencies are currently strengthening their biometric collection, storage, and matching capabilities as technologies advance and offer new opportunities to meet evolving threats to further enhance national security.

(10) This directive is designed to (a) help ensure a common recognition of the value of using biometrics in identification and screening programs and (b) help achieve objectives described in the following: Executive Order 12881 (Establishment of the National Science and Technology Council); Homeland Security Presidential Directive-6 (HSPD-6) (Integration and Use of Screening Information to Protect Against Terrorism); Executive Order 13354 (National Counterterrorism Center); Homeland Security Presidential Directive-11 (HSPD-11) (Comprehensive Terrorist Related Screening Procedures); Executive Order 13388 (Further Strengthening the Sharing of Terrorism Information to Protect Americans); National Security Presidential Directive-46/Homeland Security Presidential Directive-15 (NSPD-46/HSPD-15) (U.S. Policy and Strategy in the War on Terror); 2005 Information Sharing Guidelines; 2006 National Strategy for Combating Terrorism; 2006 National Strategy to Combat Terrorist Travel; 2007 National Strategy for Homeland Security; 2007 National Strategy for Information Sharing; and 2008 United States Intelligence Community Information Sharing Strategy.

Policy

(11) Through integrated processes and interoperable systems, agencies shall, to the fullest extent permitted by law, 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.

(12) All agencies shall execute this directive in a lawful and appropriate manner, respecting the information privacy and other legal rights of individuals under United States law, maintaining data integrity

and security, and protecting intelligence sources, methods, activities, and sensitive law enforcement information.

Policy Coordination

(13) The Assistant to the President for Homeland Security and Counterterrorism, in coordination with the Assistant to the President for National Security Affairs and the Director of the Office of Science and Technology Policy, shall be responsible for interagency policy coordination on all aspects of this directive.

Roles and Responsibilities

(14) Agencies shall undertake the roles and responsibilities herein to the fullest extent permitted by law, consistent with the policy of this directive, including appropriate safeguards for information privacy and other legal rights, and in consultation with State, local, and tribal authorities, where appropriate.

(15) The Attorney General shall:

(a) Provide legal policy guidance, in coordination with the Secretaries of State, Defense, and Homeland Security and the Director of National Intelligence (DNI), regarding the lawful collection, use, and sharing of biometric and associated biographic and contextual information to enhance national security; and

(b) In coordination with the DNI, ensure that policies and procedures for the consolidated terrorist watchlist maximize the use of all biometric identifiers.

(16) Each of the Secretaries of State, Defense, and Homeland Security, the Attorney General, the DNI, and the heads of other appropriate agencies, shall:

(a) Develop and implement mutually compatible guidelines for each respective agency for the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information, to the fullest extent practicable, lawful, and necessary to protect national security;

(b) Maintain and enhance interoperability among agency biometric and associated biographic systems, by utilizing common information technology and data standards, protocols, and interfaces;

(c) Ensure compliance with laws, policies, and procedures respecting information privacy, other legal rights, and information security;

(d) Establish objectives, priorities, and guidance to ensure timely and effective tasking, collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information among authorized agencies;

(e) Program for and budget sufficient resources to support the development, operation, maintenance, and upgrade of biometric capabilities consistent with this directive and with such instructions as the Director of the Office of Management and Budget may provide; and

(f) Ensure that biometric and associated biographic and contextual information on KSTs is provided to the National Counterterrorism Center and, as appropriate, to the Terrorist Screening Center.

(17) The Secretary of State, in coordination with the Secretaries of Defense and Homeland Security, the Attorney General, and the DNI, shall coordinate the sharing of biometric and associated biographic and contextual information with foreign partners in accordance with applicable law, including international obligations undertaken by the United States.

(18) The Director of the Office of Science and Technology Policy, through the National Science and Technology Council (NSTC), shall coordinate executive branch biometric science and technology policy, including biometric standards and necessary research, development, and conformance testing programs. Recommended executive branch biometric standards are contained in the Registry of United States Government

Recommended Biometric Standards and shall be updated via the NSTC Subcommittee on Biometrics and Identity Management.

Implementation

(19) Within 90 days of the date of this directive, the Attorney General, in coordination with the Secretaries of State, Defense, and Homeland Security, the DNI, and the Director of the Office of Science and Technology Policy, shall, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, submit for the President's approval an action plan to implement this directive. The action plan shall do the following:

(a) Recommend actions and associated timelines for enhancing the existing terrorist-oriented identification and screening processes by expanding the use of biometrics;

(b) Consistent with applicable law, (i) recommend categories of individuals in addition to KSTs who may pose a threat to national security, and (ii) set forth cost-effective actions and associated timelines for expanding the collection and use of biometrics to identify and screen for such individuals; and

(c) Identify business processes, technological capabilities, legal authorities, and research and development efforts needed to implement this directive.

(20) Within 1 year of the date of this directive, the Attorney General, in coordination with the Secretaries of State, Defense, and Homeland Security, the DNI, and the heads of other appropriate agencies, shall submit to the President, through the Assistant to the President for National Security Affairs and the Assistant to the President for Homeland Security and Counterterrorism, a report on the implementation of this directive and the associated action plan, proposing any necessary additional steps for carrying out the policy of this directive. Agencies shall provide support for, and promptly respond to, requests made by the Attorney General in furtherance of this report. The Attorney General will thereafter report to the President on the implementation of this directive as the Attorney General deems necessary or when directed by the President.

General Provisions

(21) This directive:

(a) shall be implemented consistent with applicable law, including international obligations undertaken by the United States, and the authorities of agencies, or heads of such agencies, vested by law;

(b) shall not be construed to alter, amend, or revoke any other NSPD or HSPD in effect on the effective date of this directive;

(c) is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable by law or in equity by a party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.

GEORGE W. BUSH

###

Source: The White House

CJIS ADVISORY POLICY BOARD (APB)
SPRING 2012 ADVISORY PROCESS MEETINGS
INFORMATIONAL TOPICS

STAFF PAPER

INFORMATIONAL TOPIC F

Biometric Information Sharing Update

PURPOSE

To provide an update on biometric information sharing initiatives.

POINT OF CONTACT

SSA D.A. (Andy) Loftin, 304-625-4554

FEEDBACK

Please send all questions or comments concerning this topic via the electronic feedback form on Law Enforcement Online or via the feedback form provided to the Training and Systems Education Unit at facsimile, (304) 625-5090 or e-mail: <AGMU@leo.gov>.

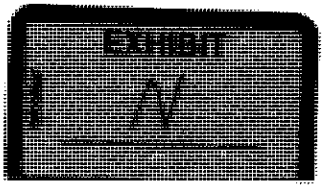
BACKGROUND

The CJIS Division's Global Initiatives Unit (GIU) has previously briefed APB Subcommittees and Working Groups on the following biometric information sharing initiatives:

- Foreign Biometric Exchange
- Preventing and Combating Serious Crime Agreements
- The Biometric Information Sharing Policy and Biometric Information Sharing Working Group

UPDATE:

Foreign Biometric Exchange (FBE): Based on previous briefings to and recommendations from the APB as well as pre-existing information sharing authorities of the FBI, the GIU's Foreign Biometric Exchange (FBE) program obtains and delivers biometric samples and related information from foreign law enforcement sources to the CJIS Division for data ingest, review, analysis, and



comparison with IAFIS. These samples are typically comprised of potential terrorist subjects, transnational criminals, or persons of national security interest. Retention of foreign biometric data in IAFIS depends on the particular agreement with the foreign agency. The GIU also assists with improving FBE capabilities by providing training and analysis to the foreign agency. Furthermore, the GIU receives and processes *ad hoc* international biometric inquiries as well as facilitates such inquiries of a foreign country's AFIS for the FBI. These *ad hoc* requests are brokered through the FBI's Legal Attaches (LEGATs) based on their authorities to share information with foreign law enforcement partners.

Through the FBE program, the CJIS Division has sharing relationships with 77 countries, in the form of both informal (*ad hoc,* verbal) agreements and formal agreements (Memoranda of Agreement, Memoranda of Understanding, or Letters of Cooperation). Collections by GIU from foreign partners range from a few records to thousands of records. To date, GIU has collected over 990,000 records from foreign partners, with over 600,000 from Afghanistan collection missions alone.

Preventing and Combating Serious Crime (PCSC): The PCSC agreements represent a White House and Congressionally-mandated joint effort between the Department of Justice, the Department of Homeland Security, and the Department of State to enter into bilateral information sharing agreements with the 36 Visa Waiver Program (VWP) countries in order to make the VWP more secure. These agreements are being implemented by the FBI at the direction of the Attorney General and will allow each party to have access to each other's fingerprint databases on a hit/no hit basis. Requests for additional information will be coordinated on a case-by-case basis, and provided through established channels (e.g., the appropriate LEGAT). All requests made under PCSC are strictly limited to Criminal Justice purposes.

Currently 20 of the 36 VWP countries have entered into PCSC agreements with the U.S.; however, none are currently sharing via the agreements. These countries include Australia, Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Portugal, Slovakia, South Korea, and Spain. Additionally one non-VWP country, Croatia, has signed a PCSC agreement.

Although Germany is not yet sharing via their PCSC agreement, the CJIS Division established PCSC connectivity with Germany's BKA in early December 2011. PCSC related sharing can commence once Germany addresses remaining internal details. Meanwhile, Spain, Estonia, Czech Republic, and Slovakia have expressed a willingness to begin sharing information under PCSC through interim measures

until the automated connections can be established. The FBI and DHS plan to travel to these countries in early 2012 to initiate the interim PCSC sharing solution.

Biometric Information Sharing Policy and the Biometric Information Sharing Working Group (BISWG): A working group has been established to approve and track the sharing of biometric extracts. The Biometric Information Sharing Policy and its Charter remain in draft form and are currently undergoing revision. However, all foreign biometric extract requests are being reviewed and approved through this process. To date, only FBI owned records have been shared via foreign extracts.

Testimony

Jerome M. Pender
Deputy Assistant Director, Criminal Justice Information Services Division
Federal Bureau of Investigation

Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law
Washington, D.C.

July 18, 2012

History of the Criminal Justice Information Services Division

Next Generation Identification

General Authority for Next Generation Identification Initiatives

28 U.S.C. § 534 authorizes the FBI to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records. 28 U.S.C. § 534 further enables the exchange of the aforementioned records and information with, and for the official use of, authorized officials of federal, state, local, and tribal criminal and non-criminal justice departments and agencies. In addition, 42 U.S.C. § 3771 authorizes the Director of the FBI to develop new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen criminal justice.

Status of Next Generation Identification Incremental Deployment

Next Generation Identification Success

In addition to increased fingerprint accuracy of 99.6 percent, deployment of Increment 1 has allowed operations to reduce the dependency on a supplemental name check, resulting in a 90 percent decrease weekly in the number of manual fingerprint reviews required by CJIS Division service providers.

Since deployment of Increment 2 (RISC), nine states—representing over 500 agencies—have begun participation in the national service; 10 additional states are in the process of implementing RISC. Over 500 transactions are processed daily with a response time of less than seven seconds and an average weekly hit rate of 6-10 percent.

Next Generation Facial Recognition

NGI Increment 4 includes a new facial recognition system. It was deployed as a pilot in February 2012 and is scheduled for full operational capability in the summer of 2014. The objective of the NGI Facial Recognition Pilot is to conduct image-based facial recognition searches of the FBI's national repository

Recent Testimonies

03.19.13 **Protecting the Nation in Today's Complex Threat Environment**
Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Headquarters.

03.13.13 **Investigating and Prosecuting 21st Century Cyber Threats**
John Boles, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation, Statement Before the House Committee on the Judiciary, Subcommittee on Crime, Terrorism, and Homeland Security, Washington, D.C.

03.13.13 **Proposal for a New Consolidated FBI Headquarters Building**
Kevin Perkins, Associate Deputy Director, Federal Bureau of Investigation, Statement Before the House Committee on Transportation and Infrastructure, Subcommittee on Economic Development, Public Buildings, and Emergency Management, Washington, D.C.

09.19.12 **The Domestic Terrorism Threat**
Michael A. Clancy, Deputy Assistant Director, Counterterrorism Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on the Constitution, Civil Rights, and Human Rights, Washington, D.C.

09.19.12 **Homeland Threats and Agency Responses**
Robert S. Mueller, III, Director, Federal Bureau of Investigation, Statement Before the Senate Committee on Homeland Security and Governmental Affairs, Washington, D.C.

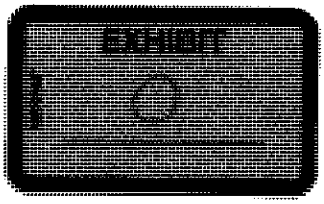
08.01.12 **Report of the William Webster Commission and the Events at Ft. Hood**
Mark F. Giuliano, Executive Assistant Director, National Security Branch, Federal Bureau of Investigation, Statement Before the House Appropriations Committee, Subcommittee on Commerce, Justice, Science, and Related Agencies, Washington, D.C.

07.18.12 **What Facial Recognition Technology Means for Privacy and Civil Liberties**
Jerome M. Pender, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law, Washington, D.C.

06.28.12 **Economic Espionage: A Foreign Intelligence Threat to Americans Jobs and Ho ...**
C. Frank Figliuzzi, Assistant Director, Counterintelligence Division, Federal Bureau of Investigation, Statement Before the House Committee on Homeland Security, Subcommittee on Counterterrorism and Intelligence, Washington, D.C.

05.21.12 **A National Security Crisis: Foreign Language Capabilities in the Federal G ...**
Tracey A. North, Deputy Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation, Statement Before the Senate Homeland Security and Government Affairs Committee, Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Headquarters, FBI

05.16.12 **Oversight of the Federal Bureau of Investigation**



Recognition Pilot are to test the facial recognition processes, resolve policy and processing issues, solidify privacy protection procedures, and address user concerns.

The Facial Recognition Pilot provides a search of the national repository of photos consisting of criminal mug shots, which were taken at the time of a criminal booking. Only criminal mug shot photos are used to populate the national repository. Query photos and photos obtained from social networking sites, surveillance cameras, and similar sources are not used to populate the national repository. The national repository is updated as transactions, including enrollments and deletions, are submitted by law enforcement users. The national repository contains approximately 12.8 million searchable frontal photos.

The Facial Recognition Pilot permits authorized law enforcement agencies to submit queries for a facial recognition search of the national repository of mug shots. The national repository can be queried by authorized criminal justice agencies for criminal justice purposes. Access to the national repository is subject to all rules regarding access to FBI CJIS systems information and subject to dissemination rules for authorized criminal justice agencies. Query requests are processed "lights out" (without human intervention), and the results are returned to the submitting agency as an investigative lead in the form of a ranked candidate list.

The investigative response provided to a submitting agency will include the number of candidates requested, in ranked order. The FBI Number/Universal Control Number of each candidate will also be returned, along with a caveat noting that the response should only be used as an investigative lead. Upon receipt of an investigative response from the FBI, the submitting agency will be responsible for conducting a full investigation of potential matching candidates.

Facial Recognition Privacy Documentation

In accordance with Section 208 of the E-Government Act of 2002, facial recognition was initially addressed by the FBI's June 9, 2008 Interstate Photo System Privacy Impact Assessment (PIA). In coordination with the FBI's Office of the General Counsel, the 2008 Interstate Photo System PIA is currently in the process of being renewed by way of Privacy Threshold Analysis (PTA), with an emphasis on facial recognition. An updated PIA is planned and will address all evolutionary changes since the preparation of the 2008 Interstate Photo System PIA.

Participating States and Agencies

Initial pilot participants are states or agencies that already have established facial recognition systems. Following completion of the pilot and implementation of the full facial recognition operating capability, additional federal, state, local, and tribal partners and agencies, with or without established facial recognition systems, will be eligible for participation.

Appropriate Use of Next Generation Identification Facial Recognition Technology

Searches of the national repository of mug shots are subject to all rules regarding access to FBI CJIS systems information (28 U.S.C. § 534, the FBI security framework, and the CJIS security policy) and subject to dissemination rules for authorized criminal justice agencies. Queries submitted for search against the national repository must be from authorized criminal justice agencies for criminal justice purposes.

Each participating pilot state or agency is required to execute a memorandum of understanding (MOU) that details the purpose, authority, scope, disclosure, and use of information and the security rules and procedures associated with piloting. Pilot participants are advised that all information is treated as law enforcement sensitive and protected from unauthorized disclosure.

Pilot participants are informed that information derived from pilot search requests and resulting responses is to be used only as an investigative lead. Results are not to be considered as positive identifications.

Current Facial Recognition Pilot Participants

In February 2012, the state of Michigan successfully completed an end-to-end Facial Recognition Pilot transaction and is currently submitting facial recognition searches to CJIS. MOUs have also been executed with Hawaii and Maryland, and South Carolina, Ohio, and New Mexico are engaged in the MOU review process for Facial Recognition Pilot participation. Kansas, Arizona, Tennessee, Nebraska, and Missouri are also interested in Facial Recognition Pilot participation.

Summary

The FBI's Next Generation Identification program is on scope, on schedule, on cost, and 60 percent deployed. The Facial Recognition Pilot, which began operation in February 2012, searches criminal mug shots and provides investigative leads. The Facial Recognition Pilot is evaluating and solidifying policies, procedures, and privacy protections. Full operational capability for facial recognition is scheduled for the summer of 2014.

Committee, Washington, D.C.

More

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

THE STATE OF HAWAII DEPARTMENT OF THE ATTORNEY GENERAL

FOR THE

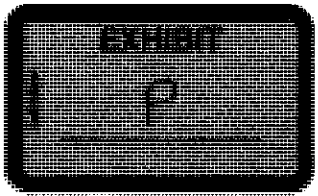
INTERSTATE PHOTO SYSTEM FACIAL RECOGNITION PILOT

GENERAL PROVISIONS

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the State of Hawaii Department of the Attorney General (HDAG), hereinafter referred to as the "Parties," is for the limited purpose of testing and piloting the FBI's Interstate Photo System Facial Recognition Pilot (IPSFRP). This MOU memorializes the Parties' understandings regarding the transmittal, receipt, storage, use, and dissemination of information relating to this piloting initiative.

2. BACKGROUND: The FBI maintains millions of digital representations of fingerprint images, features from digital fingerprint images, and associated criminal history record information in the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS provides automated fingerprint search capabilities, latent print search capabilities, electronic image storage and electronic exchange of fingerprints, criminal history and associated photos to support law enforcement and authorized civil organizations. Collectively, this data comprises the biometric content, format, and units of measurement for the electronic exchange of information that may be used for positive fingerprint identifications. Given the advances in biometric identification technology, including hardware, software, and digital imaging, it is essential that existing search capabilities be enhanced to meet authorized customer needs. The CJIS Division's Next Generation Identification (NGI) System expects to reduce terrorist and other criminal activities by implementing multiple search capabilities that will improve, expand, or create new biometric identification tools and investigative services for the FBI's user community.

The IPSFRP satisfies a subset of the NGI Interstate Photo System (IPS) requirements, and a prototype system was delivered to assist in the development of the IPS facial recognition system. Upon full implementation, IPS enhancements will: 1) expand storage capacity, thereby allowing a more robust photo repository; 2) permit photo submissions independent of arrests; 3)



full implementation, IPS enhancements will: 1) expand storage capacity, thereby allowing a more robust photo repository; 2) permit photo submissions independent of arrests; 3) permit bulk submission of photos being maintained at state and federal repositories; 4) accommodate the submission and searching of non-facial photos (e.g., Scars, Marks and Tattoos [SMTs]); 5) permit IPS photo retrieval via the National Crime Information Center (NCIC); and 6) provide facial recognition search capabilities.

It is important to note that although facial recognition technology has been under development since the 1960's, universal algorithmic approaches for facial recognition do not exist. Approaches originally tailored to low resolution, two-dimensional images have been improved to account for greater levels of resolution and three-dimensional data. The U.S. Government has performed multiple evaluations of facial recognition technology and preliminary results demonstrate that accuracy has greatly improved. Accordingly, these enhancements support the FBI's decision to enhance its photo processing capabilities in the early stages of NGI system development, to include facial recognition technology.

To address and enhance photo processing capabilities, the FBI is initiating the IPSFRP as a collaborative effort to identify user needs, provide proof of concept, establish thresholds for lights out searches at the national level and develop a useful investigative tool for the law enforcement community.

Agencies participating in this pilot program have implemented a facial recognition system for investigative, identity authentication and/or tracking purposes. In support of this initiative, the HDAG will submit images to a state/regional photo repository and the repository will provide search results to the submitting law enforcement agency. The HDAG will also request that the photo submission be forwarded to the CJIS Division, via the CJIS Wide Area Network (WAN) or other FBI approved secure web services, for comparison against the FBI's national photo repository. This pilot is designed to provide participating law enforcement agencies an automated facial recognition search of a subset of the FBI's national photo repository until full implementation of the IPS facial recognition search capability in 2014. The IPSFRP will represent a subset of the IPS repository and will be expanded and updated periodically throughout the pilot. The subset repository will not represent a real time reflection of the IPS or Interstate Identification Index (III) photo repository.

Technical specifications for the IPSFRP are derived from the CJIS Electronic Biometric Transmission Specification (EBTS) and the American National Standards Institute (ANSI) American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, & other Biometric Information.

During the IPSFRP piloting phase, relevant transactions will be analyzed by the Parties and their authorized contractors to assess system performance. In addition, the NGI IPS system design will be recording lessons learned and user input.

System availability will be limited during this initiative. Accordingly, the CJIS Division will provide advanced notice of sporadic system availability, backup recovery limitations, and failover shortfalls during the prototype phase. In addition, the CJIS Division may limit the number of transactions that will be accepted during the pilot phase.

3. AUTHORITY: The FBI enters into this MOU under the statutory authority provided by Title 28, United States Code, § 534.

4. SCOPE: This MOU applies to facial photo images provided by the HDAG and the FBI's responses.

A. The FBI will:

1. Accept one frontal facial photo submission per IPSFRP search request;

2. Search each frontal facial image against the IPSFRP national repository;

3. Provide a candidate list per each applicable IPSFRP search request. The candidate list will contain the agency's requested number (minimum of 2) of candidates, or a default number of 20 candidates if not specified by the agency, as well as a caveat message;

4. Provide a valid FBI identifier for each candidate;

5. Maintain a log of all transactions and disseminations;

6. Designate a point of contact (POC) for issues and concerns related to this initiative;

7. Conduct post processing on submitted transactions to determine system performance and miss analysis and provide results to the submitting agency; and

B. The HDAG will:

1. Submit no more than one frontal facial photo (EBTS - ANSI compliant) per IPSFRP search request via the CJIS WAN or other FBI approved secure web services;

2. Request a specified number (minimum of 2, default of 20, maximum of 50) of returned candidates;

3. Conduct a search of the III to ensure information derived from the IPSFRP candidate lists are up-to-date;

5. Disseminate FBI responses to authorized criminal justice recipients as an investigative lead;

A. Provide the CJIS Division with post processing results, such as:

1. Agency identified a subject from the candidate list and what rank.
2. Search resulted in an investigative lead.
3. Search was of no value.

B. Designate a POC for issues and concerns related to this initiative.

6. DISCLOSURE AND USE OF INFORMATION: The IPSFRP pilot search will be limited to authorized criminal justice agencies for criminal justice purposes. The IPSFRP, and the photo search thereof, is considered to be a part of the IAFIS, therefore all CJIS rules regarding access to IAFIS and dissemination/use of FBI provided information will apply. The Parties acknowledge that information involved in this initiative may identify United States persons, whose information is protected by the Privacy Act of 1974, Executive Order 12333, any successor executive order, or other federal authority. Accordingly, all such information will be treated as "law enforcement sensitive" and protected from unauthorized disclosure. Each Party will immediately report to the other Party any instance in which data received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches).

Information derived from the FBI IPSFRP search requests and resulting responses are to be used only as investigative leads. Though there are expected to be similarities between submitted images and candidate lists, results shall not be considered to be positive identifications nor considered to have active warrants. Although the emerging technology of facial recognition has made great strides over the years, facial recognition initiatives are not deemed to provide positive identifications and the Parties are prohibited from relying solely on IPSFRP search responses as the sole impetus for law enforcement action. Other indicators and factors must be considered by the submitting agency prior to making an identification.

7. FUNDING: There are no reimbursable expenses associated with this level of support. Each Party will fund its own activities unless otherwise agreed to in writing. Expenditures will be subject to budgetary processes and availability of funds and resources pursuant to applicable laws, regulations and policies. The Parties expressly acknowledge that this MOU in no way implies that Congress or the State of Hawaii will appropriate funds for such expenditures.

8. SETTLEMENT OF DISPUTES: Disagreements between the Parties arising under or relating to this MOU will be resolved only by consultation between the Parties and will not be referred to any other person or entity for settlement.

9. SECURITY: It is the intent of the Parties that the transfer of information described under this MOU will be conducted at the unclassified level. Classified information will neither be provided nor generated under this MOU.

10. AMENDMENT and TERMINATION:

A. All activities under this MOU will be carried out in accordance to the above described provisions.

B. This MOU may be amended or terminated at any time by the mutual written consent of the Parties' authorized representatives.

C. Either Party may terminate this MOU upon thirty (30) days written notification to the other Party. Such notice will be the subject of immediate consultation by the Parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

1. The Parties will continue participation, financial or otherwise, up to the effective date of termination.

2. Each Party will pay the costs it incurs as a result of termination.

3. All information, copies thereof, and rights therein received under the provisions of this MOU prior to the termination will be maintained in accordance with the receiving Party's practices.

11. ENTRY INTO FORCE, AND DURATION: This MOU, which consists of ten Sections, will enter into effect upon the signature of both Parties, will be reviewed annually, on or prior to the anniversary date, to determine whether amendments are needed, and will remain in effect until terminated or completion of the testing and piloting phase. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the Parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The preceding ten (10) sections represent the understandings reached between the FBI and the Hawaii Criminal Justice Data Center.

FOR THE FEDERAL BUREAU OF INVESTIGATION

David Cuthbertson
Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation

11/4/11
Date

FOR THE STATE OF HAWAII
DEPARTMENT OF THE ATTORNEY GENERAL

David M. Louie
Attorney General
State of Hawaii
Department of the Attorney General

11-22-11
Date

EXECUTED

MEMORANDUM OF UNDERSTANDING

BETWEEN

THE FEDERAL BUREAU OF INVESTIGATION

AND

MARYLAND DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES
INFORMATION TECHNOLOGY AND COMMUNICATIONS DIVISION

FOR THE

INTERSTATE PHOTO SYSTEM FACIAL RECOGNITION PILOT

GENERAL PROVISIONS

1. PURPOSE: This Memorandum of Understanding (MOU) between the Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS) Division, and the Maryland Department of Public Safety and Correctional Services, Information Technology and Communications Division (DPSCS-ITCD) hereinafter referred to as the "Parties," is for the limited purpose of testing and piloting the FBI's Interstate Photo System Facial Recognition Pilot (IPSFRP). This MOU memorializes the Parties' understandings regarding the transmittal, receipt, storage, use, and dissemination of information relating to this piloting initiative.

2. BACKGROUND: The FBI maintains millions of digital representations of fingerprint images, features from digital fingerprint images, and associated criminal history record information in the Integrated Automated Fingerprint Identification System (IAFIS). The IAFIS provides automated fingerprint search capabilities, latent print search capabilities, electronic image storage and electronic exchange of fingerprints, criminal history and associated photos to support law enforcement and authorized civil organizations. Collectively, this data comprises the biometric content, format, and units of measurement for the electronic exchange of information that may be used for positive fingerprint identifications. Given the advances in biometric identification technology, including hardware, software, and digital imaging, it is essential that existing search capabilities be enhanced to meet authorized customer needs. The CJIS Division's Next Generation Identification (NGI) System expects to reduce terrorist and other criminal activities by implementing multiple search capabilities that will improve, expand, or create new biometric identification tools and investigative services for the FBI's user community.

The IPSFRP satisfies a subset of the NGI Interstate Photo System (IPS) requirements, and a prototype system was delivered to assist in the development of the IPS facial recognition

system. Upon full implementation, IPS enhancements will: 1) expand storage capacity, thereby allowing a more robust photo repository; 2) permit photo submissions independent of arrests; 3) permit bulk submission of photos being maintained at state and federal repositories; 4) accommodate the submission and searching of non-facial photos (e.g., Scars, Marks, and Tattoos); 5) permit IPS photo retrieval via the National Crime Information Center; and 6) provide facial recognition search capabilities.

It is important to note that although facial recognition technology has been under development since the 1960's, universal algorithmic approaches for facial recognition do not exist. Approaches originally tailored to low resolution, two-dimensional images have been improved to account for greater levels of resolution and three-dimensional data. The U.S. Government has performed multiple evaluations of facial recognition technology and preliminary results demonstrate that accuracy has greatly improved. Accordingly, these enhancements support the FBI's decision to enhance its photo processing capabilities in the early stages of NGI system development, to include facial recognition technology.

To address and enhance photo processing capabilities, the FBI is initiating the IPSFRP as a collaborative effort to identify user needs, provide proof of concept, establish thresholds for lights out searches at the national level, and develop a useful investigative tool for the law enforcement community.

Agencies participating in this pilot program have implemented a facial recognition system for investigative, identity authentication and/or tracking purposes. In support of this initiative, the DPSCS-ITCD will submit images to a state/regional photo repository and the repository will provide search results to the submitting law enforcement agency. The DPSCS-ITCD will also request that the photo submission be forwarded to the CJIS Division, via the CJIS Wide Area Network (WAN) or other FBI approved secure web services, for comparison against the FBI's national photo repository. This pilot is designed to provide participating law enforcement agencies an automated facial recognition search of a subset of the FBI's national photo repository until full implementation of the IPS facial recognition search capability in 2014. The IPSFRP will represent a subset of the IPS repository and will be expanded and updated periodically throughout the pilot. The subset repository will not represent a real time reflection of the IPS or Interstate Identification Index (III) photo repository.

Technical specifications for the IPSFRP are derived from the CJIS Electronic Biometric Transmission Specification (EBTS) and the American National Standards Institute (ANSI) American National Standard for Information Systems - Data Format for the Interchange of Fingerprint, Facial, & other Biometric Information.

During the IPSFRP piloting phase, relevant transactions will be analyzed by the Parties and their authorized contractors to assess system performance. In addition, the NGI IPS system design will be recording lessons learned and user input.

System availability will be limited during this initiative. Accordingly, the CJIS Division will provide advanced notice of sporadic system availability, backup recovery limitations, and failover shortfalls during the prototype phase. In addition, the CJIS Division may limit the number of transactions that will be accepted during the pilot phase.

3. AUTHORITY: The FBI enters into this MOU under the statutory authority provided by Title 28, United States Code, § 534.

4. SCOPE: This MOU applies to facial photo images provided by the DPSCS-ITCD and the FBI's responses.

A. The FBI will:

1. Accept one frontal facial photo submission per IPSFRP search request;

2. Search each frontal facial image against the IPSFRP national repository;

3. Provide a candidate list per each applicable IPSFRP search request. The candidate list will contain the agency's requested number (minimum of 2) of candidates, or a default number of 20 candidates if not specified by the agency, as well as a caveat message;

4. Provide a valid FBI identifier for each candidate;

5. Maintain a log of all transactions and disseminations;

6. Designate a point-of-contact (POC) for issues and concerns related to this initiative;

7. Notify the submitting agency if a CJIS facial examiner determines (during post processing) that a probable match between the probe image and a gallery image on the returned candidate list exists; and

B. The DPSCS-ITCD will:

1. Submit no more than one frontal facial photo (EBTS - ANSI compliant) per IPSFRP search request via the CJIS WAN or other FBI approved secure web services;

2. Request a specified number (minimum of 2, default of 20, maximum of 50) of returned candidates;

3. Conduct a search of the III to ensure information derived from the IPSFRP candidate lists are up-to-date;

5. Disseminate FBI responses to authorized criminal justice recipients as an investigative lead;

A. Provide the CJIS Division with post processing results, such as:
   1. Agency identified a subject from the candidate list and what rank.
   2. Search resulted in an investigative lead.
   3. Search was of no value.

B. Designate a POC for issues and concerns related to this initiative.

6. DISCLOSURE AND USE OF INFORMATION: The IPSFRP pilot search will be limited to authorized criminal justice agencies for criminal justice purposes. The IPSFRP, and the photo search thereof, is considered to be a part of the IAFIS, therefore all CJIS rules regarding access to IAFIS and dissemination/use of FBI provided information will apply. The Parties acknowledge that information involved in this initiative may identify United States persons, whose information is protected by the Privacy Act of 1974, Executive Order 12333, any successor executive order, or other federal authority. Accordingly, all such information will be treated as "law enforcement sensitive" and protected from unauthorized disclosure. Each Party will immediately report to the other Party any instance in which data received from the other Party is used, disclosed, or accessed in an unauthorized manner (including any data losses or breaches).

Information derived from the FBI IPSFRP search requests and resulting responses are to be used only as investigative leads. Though there are expected to be similarities between submitted images and candidate lists, results shall not be considered to be positive identifications nor considered to have active warrants. Although the emerging technology of facial recognition has made great strides over the years, facial recognition initiatives are not deemed to provide positive identifications and the Parties are prohibited from relying solely on IPSFRP search responses as the sole impetus for law enforcement action. Other indicators and factors must be considered by the submitting agency prior to making an identification.

7. FUNDING: There are no reimbursable expenses associated with this level of support. Each Party will fund its own activities unless otherwise agreed to in writing. Expenditures will be subject to budgetary processes and availability of funds and resources pursuant to applicable laws, regulations and policies. The Parties expressly acknowledge that this MOU in no way implies that Congress will appropriate funds for such expenditures.

8. SETTLEMENT OF DISPUTES: Disagreements between the Parties arising under or relating to this MOU will be resolved only by consultation between the Parties and will not be referred to any other person or entity for settlement.

9. SECURITY: It is the intent of the Parties that the transfer of information described under this MOU will be conducted at the unclassified level. Classified information will neither be provided nor generated under this MOU.

10. AMENDMENT and TERMINATION:

A. All activities under this MOU will be carried out in accordance to the above described provisions.

B. This MOU may be amended or terminated at any time by the mutual written consent of the Parties' authorized representatives.

C. Either Party may terminate this MOU upon thirty (30) days written notification to the other Party. Such notice will be the subject of immediate consultation by the Parties to decide upon the appropriate course of action. In the event of such termination, the following rules apply:

1. The Parties will continue participation, financial or otherwise, up to the effective date of termination.

2. Each Party will pay the costs it incurs as a result of termination.

3. All information, copies thereof, and rights therein received under the provisions of this MOU prior to the termination will be maintained in accordance with the receiving Party's practices.

11. ENTRY INTO FORCE, AND DURATION: This MOU, which consists of eleven Sections, will enter into effect upon the signature of both Parties, will be reviewed annually, on or prior to the anniversary date, to determine whether amendments are needed, and will remain in effect until terminated or completion of the testing and piloting phase. This MOU is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any third party against the Parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

The preceding eleven (11) sections represent the understandings reached between the FBI and the DPSCS-ITCD.

FOR THE FEDERAL BUREAU OF INVESTIGATION

David Cuthbertson
Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation

11/22/11
Date

FOR THE MARYLAND
DEPARTMENT OF PUBLIC SAFETY
AND CORRECTIONAL SERVICES

Ron Brothers
Chief Information Officer
State of Maryland
Department of Public Safety
and Correctional Services

12/2/11
Date

Approved for form and legal sufficiency:

Stuart Nathan
Principal Counsel
Maryland Department of Public Safety
and Correctional Services

12/9/11
Date

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 2

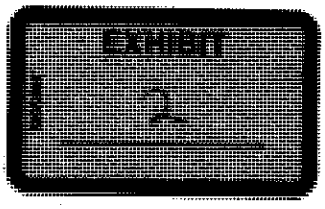
IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. CJ-2011-1469
	)	
OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. T THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,	)	
	)	
Defendants.	)	

DEFENDANTS OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, MICHAEL C. THOMPSON AND RICKY ADAMS
ANSWER TO PLAINTIFF'S PETITION

For its Answer to the Plaintiff's Petition, Defendants Oklahoma Department of Public Safety, Michael C. Thompson and Ricky Adams, in their official and individual capacities, (hereinafter "State Defendants"), deny any and all material allegations of Plaintiff's Petition unless specifically admitted herein. State Defendants further state the following:

1. State Defendants are without information as to the truth of the averments in paragraph one (1) of Plaintiff's Petition and, therefore, it is denied and strict proof thereof is demanded.



2. State Defendants admit the averment in paragraph two (2) of Plaintiff's Petition that the Oklahoma Department of Public Safety is a state entity and further admit that suing Michael Thompson and Ricky Adams in their official capacities is the same as suing a state entity, but deny that they are "Governmental entity(s)" as defined by 51 O.S. § 252(5) or that they are properly sued in their individual capacities under 51 O.S. § 256 and strict proof thereof is demanded. Furthermore, State Defendants deny the averments in paragraph two (2) of Plaintiff's Petition that the Oklahoma Religious Freedom Act at 51 O.S. §§251 et. seq. provides any private cause of action against any state employee in their individual capacity whether acting under color of state law or otherwise and denies the same and demands strict proof thereof.

3. State Defendants deny the averments in paragraph three (3) of Plaintiff's Petition and demand strict proof thereof.

COUNT 1

OKLAHOMA RELIGIOUS FREEDOM ACT OKLA. STAT. TIT. 51, §§ 251-258

4. State Defendants are without information as to the truth of the averments in paragraph four (4) of Plaintiff's Petition and, therefore, it is denied and strict proof thereof is demanded.

5. State Defendants are without information as to the truth of the averments in paragraph five (5) of Plaintiff's Petition and, therefore, it is denied and strict proof thereof is demanded.

6. State Defendants are without information as to the truth of the averments in paragraph six (6) of Plaintiff's Petition and, therefore, it is denied and strict proof thereof is demanded.

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1492

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 3

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. CJ-2011-1469
	)	
OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,	)	
	)	
Defendants.	)	

RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,

EXHIBIT

REQUEST FOR ADMISSION NO. 7: Admit that biometric information taken from Drivers License or Identification Card Applicants is accessible by Fusion Centers.

RESPONSE: Without a specific definition of "Fusion Centers" this request must be denied.

REQUEST FOR ADMISSION NO. 8: Admit that biometric information accessible by Fusion Centers may be and has been provided to State and Federal law enforcement agencies or departments upon request without a warrant.

RESPONSE: See Response to Request Number 7.

REQUEST FOR ADMISSION NO. 9: Admit that the Department of Public Safety collects biometric information from Drivers License and Identification Card Applicants without the existence of any individualized suspicion of wrongdoing and without obtaining a warrant.

RESPONSE: Admitted.

REQUEST FOR ADMISSION NO. 10: Admit that the Fusion Tag Agency, located at 1236 North Interstate Drive, Norman, OK 73072, in Cleveland County, Oklahoma, is a motor license agent/agency of the defendant Oklahoma Department of Public Safety ("DPS"), as contemplated in 47 O.S. §§ 1140 et seq.

RESPONSE: It is admitted that Fusion Tag Agency is a Motor License Agent of the Oklahoma Tax Commission, and has been approved by the Department of Public Safety to issue DL/ID cards on behalf of the Department of Public Safety.

REQUEST FOR ADMISSION NO. 11: Admit that Department of Public Safety consider's an individual's birth certificate as proof of identity.

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 4

March 18, 2011

Oklahoma State Department of Public Safety
3600 N Martin Luther King Avenue
Oklahoma City, OK. 3110

Subject: Religious objections to biometric collection for state driver's license

Dear Commissioner DPS Michael Thompson
CC: General Counsel Stephen Crise

My name is Kaye Beach. I am a resident of Oklahoma seeking to renew my Oklahoma driver's license. I have a religious objection to the collection of my biometrics particularly my facial biometric captured by the high resolution digital photo used in the state driver's license. I am not opposed to a low resolution photo on the license.

On Wed March 8, 2011 I visited Fusion Tag Agency in Norman to renew my Oklahoma driver's license. I related to the clerk at this tag agency that I have a religious objection to the capture of my facial and fingerprint biometrics and asked her what alternative might be available for me. The clerk advised me to visit the Norman DPS office and ask them as she did not know the answer to my question.

I went over to the DPS office located on N. Berry Rd. in Norman that same day and related to the DPS officer there my religious objections to the collection of my facial and finger biometrics and asked him if there was some way in which I could be accommodated. The officer asked that I leave my name and number with him so that the supervisor could return my call.

I was called back shortly by a gentleman named Steve Grunyard. He advised that he would find out the answer for me and call me back. On Friday March 10 2011 I called the Norman DPS office to see if Mr. Grunyard had any information for me. He told me that he had yet to receive a reply but would find out what he could and call me back which he did immediately.

Mr. Grunyard related to me that the collection of the finger and facial biometrics was required by law in order to receive an Oklahoma driver's license and that there was no alternative.

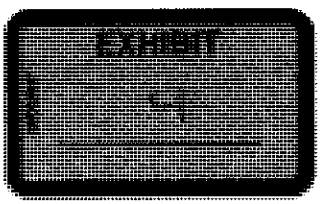
I want to be sure that I clearly understand the requirements. Are there any available administrative remedies that I can pursue that I have not pursued to this point or have I exhausted all administrative remedies.

Thank you in advance for your time and attention to this matter. I eagerly look forward to your reply.

Sincerely,

Kaye Beach

3612 Ives Way
Norman, OK. 73072
405-818-3224



IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 5

From: SKrise@dps.state.ok.us
Date: April 27, 2011 3:08:11 PM PDT
To: ladyaxiom@yahoo.com
Subject: DL photo

Ms. Beach -

I'm sorry I missed your call, but I have obtained information related to your question of whether there is an alternative to having a driver license photograph that does not capture facial recognition features, commonly referred to as biometric data. Such photographs are required by statute and the law does not provide for an alternative or exemption.

I believe this answers your inquiry, however, if you have additional questions you may contact me at your convenience. Please keep in mind that although I can answer general questions, I am not able to give you any legal advice.

Regards,

Stephen J. Krise
General Counsel
Oklahoma Department of Public Safety
3600 Martin Luther King Ave.
Oklahoma City, OK 73111
Tel: 405.425.2148
Fax: 405.425.2660

EXHIBIT
5

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 6

Traffic Citation and Information DEFENDANT'S COPY

IN THE MUNICIPAL CRIMINAL COURT OF NORMAN, OKLAHOMA

State of Oklahoma
County of Cleveland } ss.
City of Norman

532663

The undersigned, being duly sworn, upon his oath states

on or about (date) [illegible] at (time) [illegible]

at or near (location) [illegible]

County Number 14 20 within the city, county and state aforesaid:

Name (last, first, middle) [illegible]

Address [illegible] Phone Number [illegible]

City [illegible] State [illegible] Zip Code [illegible]

Birthdate (mo., day, yr.)	Age	Height	Weight	Race	Sex	Eyes	Hair
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Driver License Number	Class	CDL	Endorsement	Month/Year	State
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Employer [illegible] Phone [illegible] Did Unlawfully Operate [illegible] Park [illegible]

Vehicle Information

VIN # [illegible] MO./YR. [illegible] STATE [illegible] LICENSE [illegible]

COLOR [illegible] YR. [illegible] MAKE [illegible] MODEL [illegible] STYLE [illegible]

Commercial Motor Vehicle	Yes	No	Hazardous Material Placard
		[illegible]	☐

SPEEDING MPH in MPH Zone Pace ☐ Radar ☐ Other ☐ Lidar ☐

Other Violation:

[illegible]

AND IN VIOLATION OF SECTION [illegible]
OF THE TRAFFIC CODE OF THE CITY OF NORMAN, OKLAHOMA

I, the undersigned issuing officer, hereby certify and swear that I have read the foregoing information and know the facts and contents thereof and that the facts supporting the criminal charge stated therein are true.

[illegible] NPD [illegible]
Arresting Officer (Complainant) Address Phone

Badge # [illegible]

City Attorney

Sworn to and subscribed before me this _____ day of _____ 20____

(Deputy) Clerk, Municipal Criminal Court

Appearance Required on OR before [illegible]

at [illegible] to pay fine or to set the case for hearing before the Judge.

ADDRESS OF COURT: Municipal Court, 201 W. Gray, Bldg. B
Norman, OK 73069 (405) 366-5325

NOTICE: Release upon personal recognizance based upon a signed written promise to appear for arraignment is conditional and failure to timely appear for arraignment shall result in the suspension of the arrested person's driver's license in Oklahoma, or in the non-resident's home state pursuant to the Non-Resident Violator Compact.

WITHOUT ADMITTING GUILT, I promise to appear in said court on or before said time and place.

SIGNATURE: [illegible]

(CHECK ONE BOX ONLY)

Signed Personal Recognizance	Bond Attached	Municipal Court	Jail	Other
☒	☐ _____	☐	☐	☐

☐ JUVENILE Name of Parent or Guardian _____

Address _____

AREA ☐ business ☐ industrial ☐ school ☒ residential ☐ rural ACCIDENT ☐ PD

HIGHWAY TYPE: ☐ 1 lane ☒ 2 lane ☐ 3 lane ☐ 4 or more undivided ☐ 4 or more divided ☐ on/off ramp ☐ FATALITY ☐ PI

EXHIBIT

Norman Municipal Court
201 W. Gray, Bldg. B
Norman, OK 73069
405-366-5325

ORDER TO REAPPEAR

Name: [illegible]

Case(s): 532663

Attorney:

Penalties: 25 00.00 (50.00)

You are directed to REAPPEAR on the: 21 day of July, 20 11, at 3:00 p.m.

I have read and understand the Court Rules.

KB Initial

◇ MTA $

◇ X Arraignment

◇ Trial

Bond $

◇ Disposition

Remarks:

9/10

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 7

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH, Plaintiff, v. OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY, Defendants.	)	Case No. CJ-2011-1469

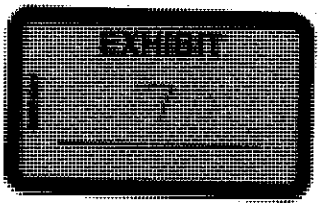
RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,



ANSWER: Photos are shared with law enforcement agencies but the finger images can only be accessed by a law enforcement agency by a court order, this information is also confidential and subject to privacy laws.

INTERROGATORY NO. 11: Does any employee or agent of the Department of Public Safety who has access to the biometric information of Applicants for Drivers Licenses and Identification Cards undergo any training, certification, specialized education, security clearance, or any other similar measure, regarding privacy protection, sensitivity of individuals' personal information, or database security? If so, please identify and explain with specificity any such measures.

ANSWER: Employees who have access to images undergo an FBI background check.

INTERROGATORY NO. 12: Identify the standard for the resolution and format of the biometric information collected from Drivers License and Identification Card Applicants.

ANSWER: DPS follows the American Association of Motor Vehicle Administrator standards.

INTERROGATORY NO. 13: Please identify the role, function, actions and input, if any, of the Department of Public Safety in the establishment of the standard for the resolution and format of the biometric information collected from Drivers License and Identification Card Applicants.

ANSWER: See the Response to Interrogatory Number 12.

INTERROGATORY NO. 14: Please identify the name, title or office, and telephone number of any person it appears at the time Defendants may call as a witness in this case, including any such person who may be called as an expert witness, along with a summary of the intended

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

Case No. CJ-2011-1489

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 8

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH, Plaintiff, v. OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY, Defendants.	)	Case No. CJ-2011-1469

RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,

EXHIBIT

Drivers License or Identification Card.

ANSWER: 47 O.S. § 6-110.2 and 47 § 6-111.

INTERROGATORY NO. 3: Please identify and individual, entity, company, organization, jurisdiction, department, agency, or any other entity that has access of any kind to the database in which Drivers License and Identification Card Applicant's biometric data is stored.

ANSWER: MorphoTrust USA

INTERROGATORY NO. 4: Please identify the individual, entity, company organization, jurisdiction, department, agency, or any other entity that provides the management, maintenance, hardware, software, logistical support, or any other type of support, regarding the database(s) in which Drivers License and Identification Card Applicant's biometric information is stored.

ANSWER: MorphoTrust USA

INTERROGATORY NO. 5: Please identify with specificity what sources of authority or law provide for, allow, require, or otherwise govern collection of, access to, and sharing of the biometric information collected from Drivers License and Identification Card Applicants.

ANSWER: There is no information sharing. The only access a law enforcement agency has to the images is via a court order.

INTERROGATORY NO. 6: Regarding the Affirmative Defenses identified in Paragraphs 6 and 7 of your Answer, please identify with specificity the sources of federal law you allege require the State of Oklahoma to gather biometric information as part of its motor vehicle licensing process and that provide a basis for your allegation of federal preemption.

ANSWER: None.

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 9

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH, Plaintiff, v. OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY, Defendants.	)	Case No. CJ-2011-1469

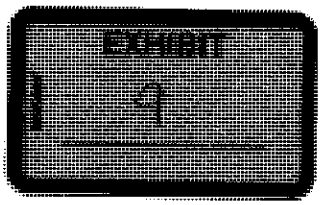
RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,



INTERROGATORY NO. 21: Please identify, including the name or title and the date entered, any agreement of any kind reached, issued or established between the Department of Public Safety and any other entity, association, corporation, department, agency, or jurisdiction, regarding the collection, storage, use, sharing or access of the biometric information of Driver License and Identification Card Applicants, including but not limited to any compacts, reciprocal agreements, memorandums of agreement, memorandums of understanding, or any other type of agreement or understanding.

ANSWER: The L-1 Contract.

RESPONSES TO REQUESTS FOR PRODUCTION

REQUEST FOR PRODUCTION NO. 1: Please produce complete copies of any and all Memorandums of Agreement, Memorandums or Understanding, reciprocal agreements, or any other type of inter-agency agreement or understanding, including any amendments or revisions thereto, reached, issued or established between the Department of Public Safety and any other agency or entity of the state of Oklahoma regarding the collection, storage, use, sharing or access of biometric information obtained by Applicants for Drivers Licenses or Identification Cards from the year 2000 to the current date.

RESPONSE: Objection. Plaintiff's request invades confidentiality concerns, violates certain privileges, requests materials that are irrelevant and are not calculated to lead to the discovery of relevant nor admissible evidence.

REQUEST FOR PRODUCTION NO. 2: Please produce complete copies of any and all Memorandums of Agreement, Memorandums or Understanding, reciprocal agreements, or any other type of agreement or understanding, including any amendments or revisions thereto, reached,

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

Case No. CJ-2011-1409

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 10

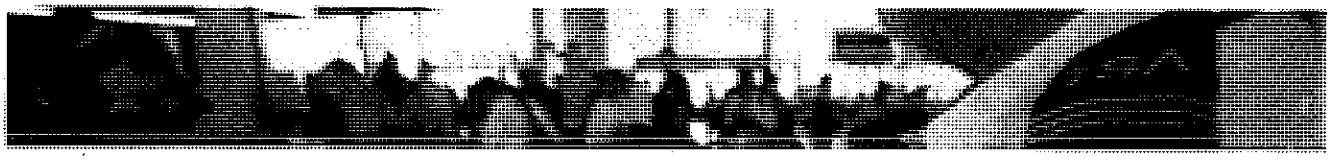
Safran/L-1 Announcement

L1 Identity

- Company
- Careers
- Contact Us
- Partners
- SAFRAN

Search... Go

- ID Issuance
- Enrollment
- ID Management
- ID Practices
- Transactions
- Investigation
- Support



- History
- Mission, Vision & Values
- Press Room
- Career Opportunities

Our History:

MorphoTrust USA, Inc. was formed when L-1 Identity Solutions was acquired in July 2011 by Safran, a global technology powerhouse in aerospace, defense, and security and an international top-tier supplier of systems and equipment. MorphoTrust is a Morpho company and part of Safran Group.

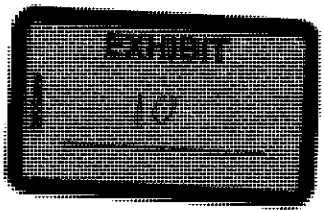
Innovation Defines Us

1958

- Implemented for Colorado the first state-issued photo driver license (DL)

1988

- Implemented the nation's first digital ID system



1990

- Implemented for California the nation's first centrally issued digital DL/ID
- Implemented for California the nation's first magnetic stripe on a digital ID
- Implemented for South Dakota the nation's first digital over-the-counter driver license solution

1992

- Designed and implemented as part of the Mexican IFE (electoral registry) program, the world's largest fingerprint-secured credential solution
- First to deploy a zero-gap central issuance process ensuring no lost/unaccounted for IDs

1995

- Implemented for West Virginia the first facial recognition secured ID

1998

- First to develop and offer breakthrough automated ID document authentication technologies

1999

- Implemented for Virginia the first "renew by Internet" system

2000

- Implemented for Massachusetts the first fully digital capture station

2002

- Implemented for Colorado the first fully operational facial and fingerprint image recognition system
- Implemented the first digital driver license in Latin America with the Costa Rica program

2003

- Implemented the first U.S. use of a Kinegram® optically-variable device for Massachusetts

2005

- First to offer a breakthrough card technology with "See, Feel, Machine-Validate" linked and layered security features for reliable authentication at places of inspection
- First to offer professional services consulting for Real ID compliance gap analysis and planning

2006

- Implemented Europe's first IDMarc security feature with the Latvia driver license program
- Implemented Ghana's first digital identity system with the Ghana driver license program

2008

- Designed and implemented for Washington state the nation's first Enhanced Driver License (EDL) for land and sea border crossing

2009

- First to implement biometric Self Service Kiosk for driver's license renewal for the Mississippi driver license program
- Received our first NASPO certification

2010

- First to offer Full Color Variable Ultra-Violet (UV) Portrait security feature with the California driver license program
- First to offer industry's first 15-year life contactless smart card for ICAO 9303 National ID and ISO 18013 driver's license standards

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

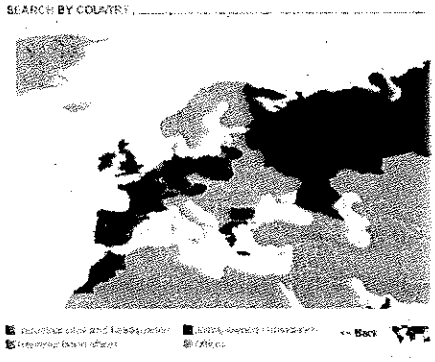
Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 11

OUR SITES

Safran is a global group, with operations on five continents. Through its design, production and service companies, as well as sales offices, Safran has established solid relationships with the world's leading prime contractors and operators, giving its customers a full range of responsive, local services.

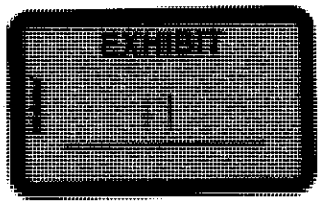


SEARCH BY COUNTRY

Select a country

SEARCH BY COMPANY

Select your company



IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

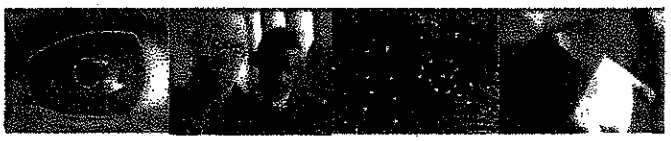
v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY C. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 12



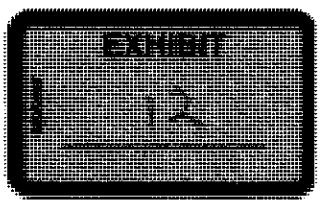
Standards

Recognizing that the development of standards is crucial to the mass adoption of biometrics, L-1 Identity Solutions actively participates in both nationally- and internationally-recognized standards initiatives:

- Technical co-editor for face recognition data interchange specifications (ANSI/INCITS 385 and ISO 19794-5, referred to by the ICAO 9303 standard for Machine-Readable Travel Documents).
- Technical co-editor for iris data interchange format.
- Contributor to minutiae- and image-based fingerprint data interchange format standards.
- Technical co-editor and active contributor to technical interfaces specifications such as CBEFF and BioAPI.
- Voting member of International Committee on Information Technology Standards M1 (biometrics section of national organization that produces technical standards for the American National Standards Institute).
- Technical expert on the US delegation to the JTC1/International Standards Organization SC37 (Subcommittee on Biometrics).
- Collaborated with ICAO representatives in travel document standards setting activities.
- Actively shaping standards via work in task groups for smart cards and biometric application profiles. Attend meetings related to the standards applicable to both our core technology and our products.
- Technical expert on the US delegation to the International Standards Organization JTC1 SC17 WG3 (Identification Cards and Personal Identification / Machine Readable Travel Documents).

In addition, L-1 Identity Solutions either currently complies or is in the process of complying with the following standards and specifications:

- **ANSI/INCITS 378 and ISO/IEC 19794-2 Minutiae-Based Fingerprint Data Interchange:**
  Facilitates interoperability and efficiency in terms of storage for minutiae-based fingerprint templates.
- **ANSI/INCITS 385 and ISO/IEC 19794-5 Face Recognition Data Interchange Format:**
  Ensures that enrolled images will meet a quality standard needed for both automated face recognition and human inspection of facial images; facilitates the use of face information in applications that have limited storage (e.g. passports, visas, driver's licenses, etc.) and allows interoperability among facial recognition vendors.
- **ANSI/INCITS 379 and ISO/IEC 19794-6 Iris Data Interchange Format:**
  Facilitates interoperability by defining a standard for exchange of iris image information. Contains a specific definition of attributes, a data record format for storing and transmitting the iris image and certain attributes, a sample record, and conformance criteria
- **ISO/IEC 19784-1 BioAPI 2.0:**
  Defines a high-level generic biometric verification and identification model allowing software applications to interface with underlying biometric services and technologies. Enables components of a biometric system to be provided by more than one vendor and to work together through a defined API (application programming interface). Open-system, consensus standard developed by a consortium of biometric vendors, integrators, and end-users over a period of several years. L-1 Identity Solutions is an active member of the INCITS M1 and ISO SC37 Technical Interfaces committees that developed and maintain this important interoperability standard.
- **ISO/IEC 19785 CBEFF:**
  Defines a data structure for creating files of biometric data that fosters interoperability between biometric components and systems. Consists of a standard header, a biometric specific memory block (BSMB), and an optional digital signature. Also includes specification for patron formats.
- **MINEX:**
  Ongoing evaluation by NIST of vendor interoperability based on the ANSI/INCITS 378 standard. Provides measurements of performance and interoperability of core template encoding and matching technologies. Developed to establish compliance for the US Government's PIV (Personal Identity Verification) Program. Minutiae Exchange (MINEX) tests are performed on an SDK submitted by a vendor. L-1's BioEngine SDK includes MINEX template creation and matching capabilities that exceed the interoperability performance provided by the version NIST evaluated in 2005 and reported on March 2006. This SDK can be used to implement MINEX functionality as part of a custom application. L-1 makes this available as an optional add-on to the workflow around an ABIS fingerprint solution.



IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1459

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 13

First Baptist
Moore

301 N.E. 27th St.
Moore, OK 73160 405-793-2600

July 2, 2012

To Whom It May Concern:

I have known Kaye Beach for over two years and as her pastor I know with absolute certainty, that Kaye Beach has strong religious objections to enrollment in a biometric identification system. Her beliefs, regarding biometrics, are based on a solid knowledge of the technology and of the Bible. In my view, as a pastor, biometrics presents a serious threat to religious freedom.

Kevin Clarkson

Dr. Kevin Clarkson

Senior Pastor

EXHIBIT
1-3

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 14

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH, Plaintiff, v. OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY, Defendants.	)	Case No. CJ-2011-1469

RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,

EXHIBIT

RESPONSE: It is admitted that an individual's birth certificate is considered a primary form of ID. Applicants must also provide a secondary form of ID.

REQUEST FOR ADMISSION NO. 12: Admit that the Oklahoma Department of Public Safety participates in and/or has access to the Electronic Verification of Vital Events (EVVE) system developed and implemented by the National Association for Public Health Statistics and Information Systems (NAPHSIS).

RESPONSE: Denied.

ANSWERS TO INTERROGATORIES

INTERROGATORY NO. 1: Please identify the Department of Public Safety's purposes(s) for refusing to provide a religious accommodation for Drivers License and Identification Card Applicants that would allow an Applicant to submit a non-biometric facial photograph and not submit fingerprints and please provide complete copies of any documents or evidence which would support the stated purposes.

ANSWER: The purpose for collecting biometric images is to verify that the person applying for a DL/ID card is that person. While there are other ways to confirm identity, there are no less restrictive means used by the Department that would verify identity to that level of certainty and with the same degree of security. Allowing exceptions would open the door for unlimited requests for exceptions and defeat the purpose of having such stringent identity verification measures. Religion does not play a role in this process.

INTERROGATORY NO. 2: Please identify all sources of authority or law, if any, the Department of Public Safety contends require it to collect and store biometric information from Drivers License and Identification Card Applicants in order to allow an Applicant to obtain a

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 15

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH, Plaintiff, v. OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY, Defendants.	)	Case No. CJ-2011-1469

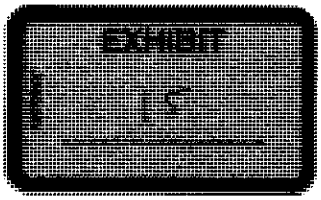
RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,



database in which Drivers License and Identification Card Applicant's biometric data is stored.

RESPONSE: Objection, due to security issues such as confidential trade secrets and proprietary information this document cannot be produced at this time.

REQUEST FOR PRODUCTION NO. 9: Please produce complete copies of any document, whether in electronic form or paper, created by any employee or agent of the Department of Public Safety which in any way pertains to the collection, storage, database accessibility or sharing of biometric information obtained from Applicants of Drivers Licences or Identification Cards.

RESPONSE: Defendant objects to this interrogatory to the extent that it is vague and ambiguous.

REQUEST FOR PRODUCTION NO. 10: Please produce complete copies of any document, whether in electronic form or paper, created by any received by any employee or agent of the Department of Public Safety from any other person or entity which in any way pertains to the collection, storage, database accessibility or sharing of biometric information obtained from Applicants of Drivers Licenses or Identification Cards.

RESPONSE: See Response to Request for Production Number 9.

REQUEST FOR PRODUCTION NO. 11: Please provide complete copies of any document containing the Department of Public Safety's stated purpose(s) or from which the stated purposes(s) are derived in whole or in part, for refusing to provide a religious accommodation for Drivers License and Identification Card Applicants that would allow an Applicant to submit a non-biometric facial photograph and not submit fingerprints.

RESPONSE: No documents to produce.

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. CJ-2011-1459
	)	
OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,	)	
	)	
Defendants.	)	

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 16

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. CJ-2011-1469
	)	
OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. T THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,	)	
	)	
Defendants.	)	

DEFENDANTS OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, MICHAEL C. THOMPSON AND RICKY ADAMS
ANSWER TO PLAINTIFF'S PETITION

For its Answer to the Plaintiff's Petition, Defendants Oklahoma Department of Public Safety, Michael C. Thompson and Ricky Adams, in their official and individual capacities, (hereinafter "State Defendants"), deny any and all material allegations of Plaintiff's Petition unless specifically admitted herein. State Defendants further state the following:

1. State Defendants are without information as to the truth of the averments in paragraph one (1) of Plaintiff's Petition and, therefore, it is denied and strict proof thereof is demanded.

EXHIBIT
1

State Defendants further deny that Plaintiff is entitled to any of the relief requested in her "Wherefore" clause or any subpart thereto either legally or factually and strict proof thereof is demanded and further state that they are entitled to dismissal of Plaintiff's action, recovery of court costs and any other relief afforded under 51 O.S. §257 against Plaintiff for filing a frivolous or fraudulent claim as anticipated by that section.

AFFIRMATIVE DEFENSES

1. Sovereign Immunity.

2. Plaintiff is not entitled to recover damages, fees or costs against State Defendants either legally or factually.

3. The possession of an Oklahoma driver's license is a privilege and not a right as anticipated by the definition of the Oklahoma or U.S. Constitutions or the Oklahoma Religious Freedom Act.

4. Fusion Tag Agency is not an agency of the State of Oklahoma and State Defendants cannot be held liable for any actions taken by them.

5. The State of Oklahoma is required by Federal law to gather biometric data as part of its motor vehicle licensing process and there is a compelling governmental interest in complying with the applicable Federal laws.

6. Federal Pre-emption.

7. The Oklahoma Religious Freedom Act does not provide a cause of action against private individuals in their individual capacities.

8. Michael Thompson and Ricky Adams are entitled to qualified immunity in their individual capacities.

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v. Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 17

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH, Plaintiff, v. OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY, Defendants.	)	Case No. CJ-2011-1469

RESPONSE TO PLAINTIFF'S FIRST DISCOVERY TO DEFENDANTS

Defendants, Oklahoma Department of Public Safety, Michael C. Thompson, Commissioner of The Oklahoma Department of Public Safety, and Ricky G. Adams, Assistant Commissioner, by and through Assistant Attorney Generals, John D. Hadden, and Kevin McClure, submit their responses to Plaintiff's First Discovery and state as follows:

GENERAL RESPONSES AND OBJECTIONS

1. Each of the following responses are made without waiving any objections Defendants, may have with respect to the subsequent use of these responses or any documents referred to herein.

2. Defendants, specifically reserve the following: (1) all questions and objections as to the competency, relevance, materiality and admissibility of responses contained herein; (2) the right to object to the use of responses set forth herein in any subsequent suit or proceeding in this action,

EXHIBIT 17

Drivers License or Identification Card.

ANSWER: 47 O.S. § 6-110.2 and 47 § 6-111.

INTERROGATORY NO. 3: Please identify and individual, entity, company, organization, jurisdiction, department, agency, or any other entity that has access of any kind to the database in which Drivers License and Identification Card Applicant's biometric data is stored.

ANSWER: MorphoTrust USA

INTERROGATORY NO. 4: Please identify the individual, entity, company organization, jurisdiction, department, agency, or any other entity that provides the management, maintenance, hardware, software, logistical support, or any other type of support, regarding the database(s) in which Drivers License and Identification Card Applicant's biometric information is stored.

ANSWER: MorphoTrust USA

INTERROGATORY NO. 5: Please identify with specificity what sources of authority or law provide for, allow, require, or otherwise govern collection of, access to, and sharing of the biometric information collected from Drivers License and Identification Card Applicants.

ANSWER: There is no information sharing. The only access a law enforcement agency has to the images is via a court order.

INTERROGATORY NO. 6: Regarding the Affirmative Defenses identified in Paragraphs 6 and 7 of your Answer, please identify with specificity the sources of federal law you allege require the State of Oklahoma to gather biometric information as part of its motor vehicle licensing process and that provide a basis for your allegation of federal preemption.

ANSWER: None.

Respectfully submitted,

KEVIN L. MCCLURE, OBA# 12767
Assistant Attorney General
Oklahoma Attorney General's Office
Litigation Division
313 N. E. 21st Street
Oklahoma City, Oklahoma 73105
Tele: (405) 521-4274 Fax: (405) 521-4518
Kevin.McClure@oag.ok.gov
Attorney for Defendants Department of Public Safety, Thompson and Adams

CERTIFICATE OF SERVICE

This is to certify that on the 18th day of June, 2012, a true and correct copy of the above and foregoing document was mailed postage prepaid, to:

M Eileen Echols
Jonathan D. Echols
Echols and Associates
9925 South Pennsylvania Ave., Suite 100
Oklahoma City, OK 73159

John W. Whitehead
Douglas R. McKusick
The Rutherford Institute
P.O. Box 7482
Charlottesville, VA 22906-7482

Kevin L. McClure

IN THE DISTRICT COURT OF CLEVELAND COUNTY
STATE OF OKLAHOMA

KAYE BEACH,

Plaintiff,

v.

Case No. CJ-2011-1469

OKLAHOMA DEPARTMENT OF PUBLIC SAFETY; MICHAEL C. THOMPSON, COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY; RICKY G. ADAMS, ASSISTANT COMMISSIONER OF THE OKLAHOMA DEPARTMENT OF PUBLIC SAFETY, IN HIS OFFICIAL AND INDIVIDUAL CAPACITY,

Defendants.

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT AS TO COUNT I, THE STATE'S VIOLATION OF THE OKLAHOMA RELIGIOUS FREEDOM RESTORATION ACT

EXHIBIT 18

...rents

A breeder document is defined as an ID document issued to support a person's identity and used to obtain another document or privilege of greater perceived value. Based on this definition, an ID document is any document containing the name of a person, and information that supports that person's claim of identity. In this light, a humble utility bill, with no security features at all, can be evidence of residence for a person to obtain a library card and get municipal services.

The most important breeder document is the birth certificate (or similar documentation). Combined with proof of residency, a birth certificate enables children to attend public school, and play sports with children of the same age. Some breeder documents are more valuable than others. If the birth certificate is the cornerstone of identity, the driving licence come a close second. In addition to bestowing driving privileges, it is widely accepted as proof of age, allowing its bearer to enter bars, buy tobacco, enter government buildings, be an airline passenger, etc. The passport is widely considered to be the ultimate ID document - it not only certifies identity, nationality and age, it also includes an image of the bearer. Yet even a passport can be used as a breeder document (to obtain a driving licence, for example).

Because breeder documents and identities are inherently linked, and because criminals continually need new identities, the weakest link in the identity generation chain is generally attacked first. Unfortunately many of these weak links are documents that are used to verify identity. Before proceeding any further, let's briefly examine why ID documents are used (and required) in the first place.

Purpose of ID documents

Identity documents are issued for three reasons.

1. As proof of identity

Someone's identity is established on the basis of his or her birth documents (the birth certificate in particular). Subsequent ID documents, such as national ID cards and passports, are usually obtained on the basis of these birth records.

2. As proof of ownership

Ownership is assigned by means of titles and deeds. While these ownership documents primarily define the object that is owned, they also tie the object to a person. They therefore provide good collateral evidence of a person's identity. It is in the interests of the state to provide records of who owns what, and highly valuable ownership records are generally well maintained.

3. Proof of privilege

Automobile and truck drivers, people who practice a profession, including lawyers, doctors, engineers, pilots, merchant mariners, beauticians and barbers, all hold licences that tie their identity to their chosen profession. Academic records and diplomas also fall in this category. Even though membership cards equally confer privileges, they are often of more limited value. It's worthwhile remembering that employee ID cards, medical insurance cards, frequent flyer cards, loyalty cards and even library cards are important means of identification within their (restricted) area of validity.

Problems arise when documents are used for purposes beyond their original function. For example, back in the late 1930s, the US authorities assigned a Social Security Card and Number to workers registered for the national retirement scheme. Because this number was unique to the person, the Social Security Number (SSN) was widely used for identification purposes far beyond the original purview, particularly as it linked many aspects of the individuals' supposedly private identity (including banking and health records). Some states used the SSN as the driver's license number.

John Mercer *is the former principal technical officer for document security matters for the US passport and visa. He chaired the Design Development Team for the US chip-enabled passport, and he served for seven years as the Chairman of the ICAO Document Content and Format Working Group, which wrote and updated international specifications for passports, visas and travel cards. He has written and presented many technical papers in the field of travel document design and security features.*