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.

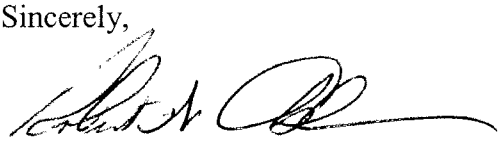
Furthermore, while the addition of biometric data to an individual's electronic file may add a layer of protection against certain types of common fraud, the inclusion of such data also greatly heightens its value for fraudulent use. That these electronic databases or networks are subject to security 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