.

Exclusive to OpEdNews:
OpEdNews Op Eds 3/12/2021 at 2:36 PM EST
H1 on 3/14/21

Follow

Become a Fan

.

REAL-IDs REQUIRED TO GET ON PLANES INVITE MAJOR PRIVACY DANGERS Should be Delayed or Scuttled as Post-Covid Travel Soon

By Robert Weiner and Adjanni Ramos

As people are preparing for post-Covid travel, "REAL-ID" is still set for October as mandatory to show TSA before getting on a plane to anywhere. It's a grave danger to privacy. It opens the door to foreign and domestic hacking with DMV in all states' employees accessing multiple personal files.

The Maryland Department of Transportation (MDOT) takes pride in being the foremost State, stating it is "proud to be the first state to be re-certified as compliant with REAL ID." Yet Maryland is a case in point, as documented in our interviews and statements from program leaders we obtained for this article.

The REAL-ID Act was controversial when it was first passed in 2005. As the time gets closer to being required for air travel and more people submit all their documents, it is more alarming. With primary and confidential information now being copied into the massive DMV files for every driver, REAL-ID has turned itself into an invitation for hacking groups and foreign governments.

Both the US House and Senate have repeatedly overlooked the dangerous aspects of volume information seeking by government.

Soon after becoming law, the REAL-ID Act received criticism from both sides of the political aisle. In 2007, Sen. Patrick Leahy (D- VT) said that because REAL-ID was slipped into a bipartisan emergency supplemental bill, it passed unopposed without senators and experts giving input on potential problems. In the *Wall Street Journal,* Leahy stated it was "more about harassing Mexican illegals."

One of its biggest complaints comes from privacy-rights advocacy groups, including the ACLU, who initiated a lawsuit against the program. The ACLU predicted it would ease access for identity thieves to steal information. They say that the problem of "insider fraud" is "not solved not is it clear there is a solution as the Act is written." (Source: ACLU "Scoreboard" of "problems commonly identified with the Real ID law."

Cyberattacks on state, federal, and corporate databases have proven that nobody is safe. Last year, after hacking private tech-firm, SolarWinds, Russian spies had accessed confidential data belonging to the Treasury Department, the Department of State, the Pentagon, and the Department of Homeland Security (DHS). The federal Office of Personnel Management (OPM), suffered its own data-breach in 2015.

Thousands of companies worldwide have had their information stolen --Target, T-Mobile, Experian -- supposed to protect the credit information of a third of all Americans-- and Marriot International's Starwood Hotels. Last year alone, over 250 companies and government agencies across the globe (half in the US) had confidential data held for ransom using some form of Malware.

When asked about the security of the files being copied from data-drives during the process of issuing an ID, a senior staffer at the Maryland DMV, Waldorf office, responded "It is only accessible to our employees. Our employees are safe." He was speechless when we said, "So was Edward Snowden."

How can it be safe to Xerox and put in universally accessible-to-DMV-employees files a copy of basically four-of these: your birth certificate, passport, unemployment, social security number, residency proof, driver's license or registration, auto insurance proof, utility bill, W-2, tax record, lease agreement, marriage certificate, a DL-32 (concerning gender change), and more? Seriously, just Xerox those into DMV files and be required to share those with other states? And if you are a migrant, there is a slew of other documents you need to bring.

When we asked about the Maryland Department of Transportation's Motor Vehicle Administration (MDOT-MVA) privacy concerns, senior spokesman Ashley Millner, Assistant Media Relations Manager for the state agency, responded on behalf of DMV:

"All Personally Identifiable Information (PII) is physically secured in MDOT-MVA databases and encrypted. The data is protected by firewalls, sensors for detecting malicious activity, Intrusion Detection Systems, and other security monitoring systems" All databases are actively audited and monitored, and access is tightly controlled" An individual's PII may not be disclosed outside of the agency, except where specifically required by state law." (Full statement below and at the link: Click Here). None of that stops an Edward Snowden from getting it.

Jay Jacob Wind, an I.T. and Data Specialist who helped develop former Vice-President Al Gore's environmental pollution data, said: "If all data is encrypted, then someone or something 'knows' the encryption algorithm, and they will test various defenses to find it and bypass the encryption algorithm, as Edward Snowden did."

The MDOT's response says nothing about preventing an individual employee from accessing a Maryland citizen's records via another State's poorly secured data-entry point. Again, remembering Edward Snowden, they can't stop an individual employee from gaining ill-intended usage. Just last year, the Texas Department of Motor Vehicles (DMV) suffered a data-breach after Vertafore - a software company with access to DMV records - was hacked due to improper storage of data information.

Thirty-one states have already shared millions of private records with each other and the DHS, to comply with the REAL-ID Act. Real-ID could take a page out of the Koch-Goldwater Privacy Act of 1974, or a Conyers-Amash 2013 congressional bill to ban bulk federal data collection without a warrant from cell phones, which failed by 13 votes but was effectively made law by a Supreme Court ban in 2018. However, as now crafted, the new Real-ID causes private information to be shared with state and federal agencies.

Much like NSA surveillance, the REAL-ID Act raises security questions towards the privacy of US citizens nationwide. It is an invitation to a future security disaster. Before COVID restrictions are lifted and people rush back to traveling, REAL-ID should be delayed or curtailed altogether without security assurances. Before it's too late and the next massive hack occurs, it's time for Congress to act.

Robert Weiner was a spokesman in the Clinton and George W. Bush White Houses. He was Communications Director of the House Government Operations Committee, and Senior Aide to Four-Star Gen/Drug Czar Barry McCaffrey and Reps. John Conyers, Charles Rangel, Claude Pepper, and Ed Koch. Adjanni Ramos is Policy and Research Analyst at Robert Weiner Associates and Solutions for Change.

Link to published article: https://www.opednews.com/articles/3/New-IDs-Required-to-Get-on-by-Robert-Weiner-Bipartisan_Information_Information_Law-210312-134.html