courier-journal
PART OF THE USA TODAY NETWORK

Real losses from REAL ID compliance

Jim Harper

October 16, 2016

When the U.S. Department of Homeland Security rejected Kentucky's application for an extension of time to comply with the REAL ID Act this week, it set up some important decisions for the Kentucky General Assembly. Frankfort will soon decide whether or not to permanently cede authority over state licensing policy to Washington, D.C. The legislature and governor will also decide whether personal information about Kentucky drivers will be shared across a nationwide network of databases. Rather than worrying about using their drivers' licenses at military bases and airports, Kentuckians' might want to worry about the privacy risks of being part of the DHS's national ID system.

Complying with REAL ID would have lasting negative implications for Kentucky. For one, the legislature would permanently lose authority over driver licensing policy. This traditional state prerogative - deciding who can be licensed, on what terms, and based on what documentation - would become the province of DHS officials in Washington, D.C., who could choose any policy that the national government preferred. This is not a power the state could ever take back.

The most direct impact on state power, though, would be felt in Kentucky's pocketbooks. If Kentucky becomes a REAL-ID compliant state, Kentucky will pay for the licensing policies that the federal government dictates. Untethered by budgetary constraints - that is, free to spend other people's money - DHS will predictably produce increasingly costly and inconvenient licensing requirements year over year. That will drive up the cost of the driver's license for Kentuckians and drive down the discretionary funds available to the legislature. The DHS's own cost estimate, issued in 2008, found that implementing REAL ID would cost $17 billion nationally, with the bulk of those costs falling on states and individuals.

But the non-monetary costs are some of the most important, including the privacy and security risks of complying with REAL ID. Those risks are created by the nationwide data-sharing network that the federal law requires.

Section 202(d)(12) of the REAL ID Act requires compliant states to "[p]rovide electronic access to all other States to information contained in the motor vehicle database of the State." That means that any data in Kentucky's driver databases might be shared with any other department of motor vehicles. Kentuckians' data would only be as secure as the least secure DMV in the country. In a data breach, foundational identity data could be made available to hackers and identity fraudsters.

Weekly, it seems, news reports come in about data breaches affecting both public and private entities. Were that to happen to the national ID network that DHS is building, the country's entire identity infrastructure could be compromised.

Perhaps because it is such an affront to privacy and data security, the DHS has temporarily written the data-sharing requirement out of the law. The regulation the department issued makes little reference to it. Data-sharing is not one of the requirements that the agency considers when it decides whether states are "compliant" with its ad hoc standards or not. And the agency consistently denies that this is a national ID program. But the clear terms of the law, quoted above, show that it is.

Sometime after DHS wins compliance commitments from a sufficient number of states, it will revive the data-sharing requirement in the law. DHS will again go around the country, state by state, and threaten state officials. "Open up your databases," they will say, "or we will have to refuse your licenses at military bases, federal facilities and TSA checkpoints."

In the first few years after the REAL ID Act became law, states around the country rejected this unfunded federal mandate in what came to be known as the "REAL ID Rebellion." When a deadline rolled around, DHS would predictably move it back for all states at the same time. But in the last few years, DHS has instituted a divide-and-conquer strategy. It selects key states and threatens them with penalties for non-compliance. Whether the penalties ever come, this goads states into committing to national ID compliance.

This time, DHS has picked Kentucky for special mistreatment. The question is whether DHS can pick off state power, power over the state's pocketbook, and the power to control Kentuckians' personal information. The people of Kentucky might prefer a legislature that works for them rather than for DHS officials in Washington, D.C.

Jim Harper is a senior fellow at the Cato Institute.