Written by **Bob Adelmann** on February 20, 2014

ICE Solicits, Withdraws Bid for National License Plate Database

The pushback from the Immigration and Customs Enforcement (ICE) agency's request for bids to build a national database of all license plate data now being collected elsewhere across the country was immediate and, for the moment at least, effective: Within a week the agency withdrew its request.

ICE said such a national database would just make its job of tracking illegal immigrants easier, that it "could only be accessed in conjunction with ongoing criminal investigations or to locate wanted individuals," and besides, the data would reside outside the government itself, safe from prying eyes.

Those justifications were met with loud guffaws, first by the Electronic Frontier Foundation (EFF), then by the ACLU, and finally by "The Judge," Andrew Napolitano. Said EFF staff attorney Jennifer Lynch, "Ultimately, you're creating a national database of location information. When all that data is compiled and aggregated, you can track somebody as they're going through their life." ACLU staff attorney Catherine Crump added: "This is yet another example of the government's appetite for tools of mass surveillance."

Judge Napolitano said such a move is unconstitutional:

> The Constitution establishes a bar over which the government must get before it can commence any investigation about anybody.
>
> Law enforcement is not allowed to use its powers for no reason, or on a hunch or a whim. It has to have a reason that they can articulate as to who did what wrong before they can start investigation.

One week after the solicitation for bids went out, it was withdrawn, the government exercising its usual penchant for misdirection and persiflage. In an e-mail Gilliam Christensen, a deputy press secretary at ICE, wrote:

> The solicitation, which was posted without the awareness of ICE leadership, has been canceled.
>
> While we continue to support a range of technologies to help meet our law enforcement mission, this solicitation will be reviewed to ensure the path forward appropriately meets our operational needs.

Uh huh: No one here is responsible for publishing the solicitation, so no one is to blame. Besides, top people weren't kept in the loop on this, so they can't be held responsible. Anyway, we're going to take another look at it but, don't worry, we'll be back.

Back in 2010, long before ICE decided to collate, correlate, organize, capture, and aggregate all license plate data into one easily accessible place, Mike Katz-Lacabe learned firsthand just how invasive and broad was the data the surveillance state was collecting on him. A computer geek living in San Leandro, California, Katz first learned about how local police were invading his privacy and decided to file a request under the California Public Records Act to learn just how much they already knew about him.

The report he received contained 112 photographs of him driving either his Toyota Tercel or his Prius. Said Katz:

> I was surprised there were some pictures where I could actually identify people. Here's one where I'm driving. Here's me in my Cal shirt.

The photos showed him driving along Estudillo Avenue near the library, another parked at a friend's house, and still another out in front of his favorite coffee house. There was even a photo of him and his two daughters exiting his car when he pulled into his driveway. Katz added: "Why are they keeping all this data? I've done nothing wrong."

They're keeping it, Mr. Katz, because they can. Katz should consider himself lucky. Only when the *Minneapolis Star Tribune* published a map of the locations Mayor R.T. Rybak's vehicle was frequently located did the mayor discover he was also being targeted randomly by local police.

All of this is old news to the ACLU, which undertook a massive effort to learn just how invasive and extensive such auto-tag surveillance was around the country. It asked 587 local police departments and state agencies to determine how much data they were collecting from auto-tag cameras, how they were using it, and how long they were keeping it. Half of the agencies complied with the ACLU's request, inundating the group with 26,000 pages of data. From that, the ACLU uncovered enormous reams of data being recorded and kept on millions of people. The problem is that the auto-tag cameras don't discriminate. They are "typically programmed to retain the location information and photograph of every vehicle that crosses their path, not simply those that generate a hit." A hit occurs when a particular license number corresponds to one in any of the 20 already-existing data bases across the country absorbing such data. Said the ACLU:

> Together these databases contain hundreds of millions of data points revealing the travel histories of millions of motorists who have committed no crime….
>
> [They represent] a single, high-resolution image of our lives.

As the Supreme Court noted in its 2010 ruling United States v. Maynard:

> A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one fact about a person, but all such facts.

In its report the ACLU created some scenarios exposing how such data could be used in the hands of those with an agenda:

> A citizen group organizes a protest calling for an end to the "war on terror." Many people show up. The police department uses a license plate reader-equipped police cruiser to scan the license plates of all who park in a nearby parking lot to attend the protest. They then investigate these individuals, showing up at their places of employment to ask questions about their backgrounds.

Or this:

> A journalist at a small newspaper publishes a series of explosive stories charging local police officers with planting drugs on suspects in order to meet arrest quotas. The stories are clearly based on insider information, so police officials park a license plate reader outside the newspaper's office and check each car that drives by against a list of police officers' license plate numbers. When they see an officer paying visits to the newspaper, they fire him on a technicality.

Or this:

> The mayor of a medium-sized Midwest city is attempting to fight off the first major challenge to his position in over 20 years, and hears a rumor that his challenger has a mistress. He asks his police commissioner to analyze historical license plate reader data for his challenger's license plate, and is able to confirm that he regularly visits the home of a young, single woman after 10 p.m. The mayor anonymously tips off a local journalist, who confirms the affair and publishes a front-page story exposing it.

These are just conjured scenarios. For Kerry Diotte, it was real. When Diotte, a reporter for the *Edmonton Sun* newspaper, wrote an article criticizing Edmonton police for using traffic cameras to generate revenues, the police turned on him, using its data base in an attempt to monitor his habits, find out his weaknesses and failings, hoping to find a reason to arrest him. For Diotte it ended well, with the police chief and several officers being fired and Diotte being exonerated.

But the threat remains. In Brookline, Massachusetts, locals became incensed at the invasion of privacy threatened by unrestricted availability of such private data, and created a grassroots effort to balance the need for privacy with the use of an otherwise helpful tool in criminal investigations. Here are the relevant portions of that story from Kade Crockford, director of the Technology for Liberty Project at the ACLU of Massachusetts:

> Massachusetts has a fairly unique town government structure, but people who live in states with strong town or county powers can follow the Brookline model to great effect. Our organizing followed some basic principles:
>
> First, find out what's going on. In order to do that, we did a cursory web search to see what kind of information existed in the public sphere. We found that the state had recently received funding from the federal government that it planned to use to purchase license plate readers for city and state law enforcement.
>
> Alarmingly, the state website describing the grant said that all police departments that received funds would be required to submit all captured license plate data to the state criminal justice database.
>
> That alerted us to a serious threat: the possibility that the state would amass detailed records of our driving habits, all without warrants or any probable cause whatsoever.
>
> Next we filed a public records request to find out which cities and towns had received funding from the state. Upon receiving those records, we learned that Brookline — an affluent Boston suburb with a higher-than-average ratio of privacy advocates to residents — was on the list.
>
> We then began the next phase of our organizing: getting the word out. Working with activists in Brookline, we penned op-eds in the local newspapers, warning residents and town government officials that if the police accepted the state grant money, all of their motoring movements would be shared with the state, and the city would lose control over the data forever. It made for a

convincing argument, and the local government held a hearing about the matter.

The last step was turning out like-minded people to join us in raising concerns. We asked interested residents to come to the hearing to deliver testimony arguing that the local government should reject the license plate reader grant.

After much back and forth with the town government and lots of discussion in the local media, Brookline's Board of Selectmen eventually agreed with us and the town's privacy advocates: The plan's risks outweighed its benefits. The grant was voted down.

Ultimately, our arguments had been so winning that even the chief of police — a major advocate of license plate reader technology — agreed that it was probably best to skip the state's grant, since it was tied to data sharing requirements that put Brookline residents at risk for privacy violations.

It's clear that the surveillance state will continue to invade privacy until such privacy becomes a relic of history. It's also clear that such efforts are reversible as the Brookline example shows. The announcement and immediate reversal of the ICE proposal earlier this week is just one more example of how an informed electorate can push back against the state's agenda.

A graduate of Cornell University and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at www.LightFromTheRight.com, primarily on economics and politics. He can be reached at badelmann@thenewamerican.com.*