Smile, you are on (government) candid camera

Posted At : September 1, 2012 6:50 PM | Posted By : Michael Smith
Related Categories: 2012

In many places in the US *every* car moving on certain roads is tracked by license plate reading cameras. And the car's driver and passengers photographed. The data is not restricted to suspected criminals, unless you believe that every citizen is potentially a criminal... And all the data is kept for future searches, for years into the future. Just in case the government needs some evidence of you wrong doing, driving in a suspicious pattern. Maybe going by a "known" drug area or a "known" anti-government group.

The same is true in London, UK and much of Europe

Check your calendar, perhaps you missed something, the year might be 1984...

> Tag readers are cameras that can be stationary, mounted on poles or traffic signals. Also they can be put on cruisers and vehicles. They can also be hidden. Their function is to take images of passing vehicles, and they have an extraordinary capacity technologically to be able to do so, and to use optical character recognition to identify the license plate number. The images may include optionally images of the occupants, the driver and passengers, as well. It takes that data, along with the GPS location of the vehicle, the date, the time, etc., and then stores it, matches up the data, and can send it to a centralized data warehousing center where they can log, historically, the movement of your own vehicle as it has passed through and silently triggered any one of the many thousands of tag readers that over the past few years have been put in place without very much public discussion or debate.
>
> TG: Where are they? Cities and towns and everywhere at this point?
>
> CM: Yes. In fact, the federal government has, over the past number of years, embarked on a campaign to use federal funds to either subsidize or to give money for tag readers ostensibly for law enforcement purposes all across the country. In Utah, they were presented in much of the same way that the government and law enforcement presents these surveillance technologies; they roll them out as an innocuous way to take a snapshot of passing vehicles and compare them to a stolen vehicle list. Well, yeah, that's part of what it does, but then in Utah they came to understand that that was only a fraction of the functionality of the tag readers that were being offered to them for free. And they expressed shock that the government was actually intending to take a historical record of all the cars that passed through on their interstate and send it off to a data warehouse, which is physically located in Northern Virginia, in Merrifield.
>
> TG: Right. Because the data warehouse in Virginia would be really concerned about stolen cars in Utah, right?
>
> CM: Well, exactly. And you know, one of the great concerns, or a number of important elements here -- there are virtually no real hard restrictions on the retention of this data, or on the use of the data. And when you aggregate it, the real risk to privacy, the greatest risk to privacy comes through both the historic accumulation of data so that it's not just a snapshot, but actually a history.
>
> But also, when you aggregate it and cross-reference it with other information such as a person's credit card transactions, what they purchased, when they purchased and why, you can really create a comprehensive profile of a person's activities, their associations, even really a personality profile on them. Imagine, they know more about you than you probably know about yourself when they take into consideration your movements, your purchases as reflected in card databases, your credit card transactions, each of which record the time, location, nature of your transactions. And that and your cell phone data, well, what's left?
> ...
>
> When you aggregate this information and know, for example, who has been parked near an abortion clinic, who has attended a political organizing meeting, and for an individual, what are the chain of activities that you have engaged in? That information does not belong to the government. That is just a clear violation, an intrusion of personal privacy.
>
> There is always a pretext, there is always an explanation. There is always some boogie man to turn to, a threat of violence. All of the counterintelligence program disruption activities of the Civil Rights and anti-war movements of the 1960s and 1970 period, early '70s were justified by the government as necessary to

prevent acts of violence, and to further law enforcement. So that's what they do here. They say, "Look, this can help prevent acts of violence. If we knew this, we could prevent a terrorist attack If we knew this, we could prevent lawlessness, we could track stolen vehicles." There are a lot of pretexts for it.

But ultimately, when you look at the design of these systems, the systems are really massive intelligence networks. A lot of these uses do not require the massive retention and data warehousing that municipalities in the federal government are engaged in. If you look to identify whether a vehicle that just passed a tag reader, for example, is a stolen vehicle, they can send in an alert and have an officer pull it over. You don't need to capture and record every single vehicle's license plates and possibly the photos of the occupants, and then move that into a data warehouse for archiving purposes. That's not necessary.

Full article at alternet