ICE Tracking Massive Number Of License Plates Across America

License plate readers have become ubiquitous with multiple agencies and police departments creating billions of scans. Furthermore, the data is being aggregated for use in a single giant database that will allow the movement of a single car to be mapped. TN Editor

The news that Immigrations & Customs Enforcement is using a massive database of license plate scans from a private company sent shockwaves through the civil liberties and immigrants' rights community, who are already sounding the alarm about how mass surveillance will be used to fuel deportation efforts.

The concerns are certainly justified: the vendor, Vigilant Solutions, offers access to 6.5 billion data points, plus millions more collected by law enforcement agencies around the country. Using advanced algorithms, this information—often collected by roving vehicles equipped

with automated license plate readers (ALPRs) that scan every license plate they pass—can be used to reveal a driver's travel patterns and to track a vehicle in real time.

ICE announced the expansion of its ALPR program in December, but without disclosing what company would be supplying the data. While EFF had long suspected Vigilant Solutions won the contract, The Verge confirmed it in a widely circulated story published last week.

In California, this development raises many questions about whether the legislature has taken enough steps to protect immigrants, despite passing laws last year to protect residents from heavy-handed immigration enforcement.

But California lawmakers should have already seen this coming. Two years ago, The Atlantic branded these commercial ALPR databases, "an unprecedented threat to privacy."

Vigilant Solutions tells its law enforcement customers that accessing this data is "as easy as adding a friend on your favorite social media platform." As a result, California agencies share their data wholesale with hundreds of entities, ranging from small towns in the Deep South to a variety of federal agencies.

An analysis by EFF of records obtained from local police has identified more than a dozen California agencies that have already been sharing ALPR data with ICE through their Vigilant Solutions accounts. The records show that ICE, through its Homeland Security Investigations offices in Newark, New Orleans, and Houston, has had access to data from more than a dozen California police departments for years.

At least one ICE office has access to ALPR data collected by the following police agencies:

- Anaheim Police Department
- Antioch Police Department
- Bakersfield Police Department
- Chino Police Department

- Fontana Police Department
- Fountain Valley Police Department
- Glendora Police Department
- Hawthorne Police Department
- Montebello Police Department
- Orange Police Department
- Sacramento Police Department
- San Diego Police Department
- Simi Valley Police Department
- Tulare Police Department

ICE agents have also obtained direct access to this data through user accounts provided by local law enforcement. For example, an ICE officer obtained access through the Long Beach Police Department's system in November 2016 and ran 278 license plate searches over nine months. Two CBP officers further conducted 578 plate searches through Long Beach's system during that same period.

It's important to note that ALPR technology collects and stores data on millions of drivers without any connection to a criminal investigation. As EFF noted, this data can reveal sensitive information about a person, for example, if they visit reproductive health clinics, immigration resource centers, mosques, or LGBTQ clubs. Even attendees at gun shows have found their plates captured by CBP officers, according to the Wall Street Journal.

Police departments must take a hard look at their ALPR systems and un-friend DHS. But the California legislature also has a chance to offer a defense measure for drivers who want to protect their privacy.

Update: The California Senate voted down S.B. 712 on January 30, 2018.

S.B. 712 would allow drivers to apply a removable cover to their license plates when they are lawfully parked, similar to how drivers are currently allowed to cover their entire vehicles with a tarp to protect their paint jobs from elements. While this would not prevent ALPRs from collecting data from moving vehicles, it would offer privacy for those

who want to protect the confidentiality of their destinations.

Before the latest story broke, S.B. 712 was brought to the California Senate floor, where it initially failed on a tied vote, with many Republicans and Democrats—including Sens. Joel Anderson (R-Alpine) and Scott Wiener (D-San Francisco)—joining in support.

Unfortunately, several Democrats, such as Senate President Kevin de León and Sen. Connie Leyva, who have positioned themselves as immigrant advocates, voted against the bill the first time around. Others, such as Sens. Toni Atkins and Ricardo Lara, sat the vote out.

The Senate has one last chance to pass the bill and send it to the California Assembly by January 31. The bill is urgently necessary to protect the California driving public from surveillance.

Californians: join us today in urging your senator to stand up for privacy, not the interests of ICE or the myriad of financial institutions, insurance companies, and debt collectors who also abuse this mass data collection.

Read full story here…

Scientists Lecture On Global Warming In Davos… Buried In Snow

Technocrat scientists pushing global warming have no idea how foolish they look as they preach warming disaster while buried in frigid snow. They are sure their science is settled and deniers are all wrong. TN Editor

Scientists have once again set up a mock Arctic base camp to educate world leaders about man-made global warming at the World Economic Forum in Davos, Switzerland.

Climate scientists hope their mock camp illustrates how global warming could impact the Arctic, but the "Gore effect" may make it harder to get the message across. Davos has seen frigid temperatures along with about six feet of snow in the last six days.

CNBC reported that "heavy snow had already blocked the rail line through the Alps from Zurich, and villages along the route were at the highest level of avalanche alert." Davos visitors were forced off trains and onto "a half-hour bus trip on back roads around the blockage and then loading them onto a crowded red commuter train that ran the rest of the way into Davos."

The camp was first set up by climate scientists, including those from the British Antarctic Survey, at Davos in 2017 to "convey that long-term negative changes in the Arctic pose serious socio-economic risks to the rest of the world," according to a January 2017 World Economic Forum blog post.

Scientists hope to convince global leaders to take drastic actions to fight global warming. Climate has been a major topic of past Davos meetings, and even though most of the world signed onto the Paris climate accord, experts fear it's not enough to stop "dangerous" warming.

Indeed, high-profile celebrities and politicians have visited the camp in

the past, including former Vice President Al Gore. Fashion designer Stella McCartney visited the camp this year, obviously bundled up to stay warm in the midst of all that snow.

Read full story here…

Everything You Need To Know About A Nationalized 5G Wireless Network

It might be that the story about nationalizing 5G was a trial balloon that turned into a lead balloon, but it doesn't mean that 5G isn't racing ahead like a freight train. Corporate cellular providers like AT&T, Sprint, Verizon, etc., will all build their own 5G networks, resulting in more towers and more radiation. 5G is so fast that it will revolutionize the Internet of Everything, allowing real-time transmission of data. TN Editor

Over the weekend, Axios reported on an unusual proposal from the National Security Council: the US government should build its own 5G

network. Axios obtained an internal memo and Powerpoint Presentation created by a senior NSC official and distributed to officials in other federal agencies.

The news has caused a wave of reaction across agencies and the political spectrum, in part because 5G is such a hyped technology with a lot of hopes riding on it, and in part because nationalizing a traditionally private industry is a big, sweeping change. We looked into what it all means and whether it's actually likely to happen.

What is a nationalized 5G network?

Simply put, a 5G—or fifth generation—network would use high-frequency airwaves to distribute wireless data. This would allow much faster speeds—up to 20Gbps—versus the current 4G maximum bandwidth of 1Gbps. 5G networks will be necessary for things like driverless cars and the expanded Internet of Things to function. But building a 5G network takes time and money because it requires an almost entirely new infrastructure of towers and equipment. Because 5G operates on a higher frequency, it's more easily disrupted by things like weather, trees, and buildings. That means a functional 5G network would require cell bases every 100-200 meters.

Though private telecom companies are racing to be the first to build 5G networks in the US, the NSC proposal suggests that the federal government should take the reigns and just build the infrastructure itself. The government would then own the network, and it could lease the use of the network to private companies.

Why would the government want to do that?

The main arguments presented in the NSC proposal are that having government ownership of the network would allow the US to get its network built first, before other global powers, like China, have a chance to dominate the market. Chinese telecom giant Huawei is already making great strides towards a 5G network.

"China has the ability to just order the rollout and that network would be large enough to create economies of scale allowing Huawei to develop

the necessary handsets and networking equipment, which they would sell to the rest of the world," Harold Feld, senior vice president at DC-based digital rights group Public Knowledge, told me.

The Powerpoint presentation outlines this early in the document, stated that China "has achieved a dominant position in the manufacture and operation of network infrastructure," and that the United States is "losing, but…we can make a fundamental change. Otherwise, China will win politically, economically, and militarily."

There's also a concern about cybersecurity and whether private companies will be able to create networks that can keep out hackers.

"It basically boils down to: 'If we, the people in charge of national security, dictate the terms on which this network is built, we will damn well make sure it is secure,'" Feld said.

How are different groups reacting?

The thing about this proposal is a nationalized telecom infrastructure is not necessarily a GOOD or BAD idea, but the idea of the federal government—rather than private industry—owning such a large communications infrastructure project would be a significant change in how wireless networks operate today, and is surprising coming from a conservative administration that nominally champions the free market. Many prominent voices have criticized the idea, question whether it would allow the government the ability to more easily spy on citizens' communications, censor how we use the network, or disrupt the free market.

Read full story here…