The American Conservative

Dirt Boxes: The Newest Government Tool for Warrantless Privacy Invasion

Dan King

December 28, 2017

That plane flying overhead could very well be scooping up your most intimate data, especially if you live in Texas. The Texas National Guard has reportedly equipped two of its RC-26 military aircraft with cell phone data-collecting dragnets, known as dirt boxes. The ability of government agencies to add new modifications to their aerial surveillance capabilities without any real oversight should sound an alarm for all Americans, not just those who live in the Lone Star State.

Dirt boxes are one of the top cell site simulators, devices that mimic cell towers and fool phones into sharing data with them. While the Department of Justice (DOJ) has advised agencies not to collect the actual content of phone calls or messages without warrants, the simulators have the ability to do so. Additionally, these tools can record and listen to calls as they occur, block phones from sending and receiving calls, and collect metadata and geolocation data, allowing law enforcement officials to track the exact location of any phone user in the area. Just the metadata alone can paint a very specific picture of the individual sending it.

"They indiscriminately gather information on countless innocent people who have the misfortune of being in the vicinity of a suspect target," said Stephanie Lacambra, criminal defense staff attorney at the Electronic Frontier Foundation. "They also disproportionately burden minority communities."

The D.C. Court of Appeals recently ruled that law enforcement use of cell site simulators—which were originally intended for terror and military investigations—without a warrant violates Americans' Fourth Amendment rights. However, law enforcement agencies around the country have routinely flouted such orders, deploying the devices in a variety of non-terror and non-military cases without warrants. For example, the NYPD has used cell site simulators without a warrant more than a 1,000 times since 2008.

Further complicating matters, the Texas National Guard is not actually a law enforcement agency, but a military entity, so it's unclear whether privacy protections apply to simulators under their control.

"Because the National Guard is under the jurisdiction of the Department of Defense, they are not necessarily bound by the policies regulating cell site simulator use promulgated by the Department of Justice and Department of Homeland Security," Lacambra said.

When pressed by the *Texas Observer* about what measures, if any, were being deployed to protect Americans' civil liberties, Texas National Guard officials declined to answer.

They also neglected to give specifics as to what the simulators are being used for. However, the contract between the Texas National Guard and Digital Receiver Technology, the producer of the dirt box, shows that planes equipped with the technology are employed in counternarcotics work. Digital Receiver Technology did not respond to a request for comment on this story.

Lacambra said she believes the devices are being used for counternarcotics, but added, "I am skeptical that they are being limited to that use. I think it is reasonable to suspect that these cell site simulators are being deployed as tools in general domestic criminal and immigration investigations along the border and throughout the state of Texas monitored by the National Guard."

According to the American Civil Liberties Union (ACLU), as many as 26 different states use cell site simulators at either the local or state level, and 13 federal agencies snoop with the fake towers as well. But, as is the case in Texas, the use of the dirt boxes are frequently clouded in secrecy, due to non-disclosure agreements between the devices' producers and law enforcement agencies. Local police departments have also been vague on the rules and regulations for the use of simulators.

Texas's airborne version of phone snooping comes just months after a group of Republicans, led by Senator John Cornyn, introduced a bill, the "Building America's Trust Act," that would put the area near the border under constant drone surveillance. If passed, it would require unmanned drones to scour the border 24 hours a day, five days a week. That's in addition to a required 95,000 hours of manned surveillance flights at the border per year, and a host of other overreaching provisions in the bill, including facial recognition software and cell phone data collection at border crossings. Travelers would be required to step aside to kiosks that would scan their faces with cameras when they arrive, and again when they leave the country, to make sure they don't overstay their visas. However, when tested, the biometric kiosks—which aren't perfect at detecting identities—have also been used to scan the faces of Americans to confirm their citizenry. Cornyn's bill has been introduced and placed on the Senate's legislative calendar for a later vote.

The increased reliance on aerial surveillance, combined with the emergence of more powerful technologies such as cell site simulators, spells trouble for civil liberties, as oversight and regulations often lag far behind technological progress.

As the Cato Institute's Matthew Feeney put it in a 2016 policy analysis, "State and federal lawmakers should take it upon themselves to provide more privacy than the Supreme Court's aerial surveillance rulings and tackle the challenging task of allowing law enforcement to effectively use drones without threatening privacy."

Lacambra added that current policies regarding cell site simulators "carry no enforcement mechanisms to punish law enforcement for violating the terms of the policy."

More checks are drastically needed for the use of cell site simulators and aerial surveillance. A non-binding order from the Department of Justice and a Fourth Amendment ruling from the D.C. Court of Appeals does nothing without more localized focuses on transparency and accountability.