Google’s Wing warns new drone laws ‘may have unintended consequences’ for privacy



This past week, the US government made the single biggest, most impactful set of changes to drone law we’ve yet seen — ruling that almost every drone in US airspace will need to broadcast their locations, as well as the location of their pilots, in order to “address safety, national security, and law enforcement concerns regarding the further integration of these aircraft into the airspace of the United States”.

Google (technically, Alphabet) isn’t too happy about those new rules, as it turns out. The company’s drone delivery subsidiary Wing wrote a somewhat fearmongering post (via *Reuters*) titled “Broadcast-Only Remote Identification of Drones May Have Unintended Consequences for American Consumers,” which argues that the FAA’s decision to have drones broadcast their location might let observers track your movements, figuring out where you go, where you live, and where and when you receive packages, among other examples.

“American communities would not accept this type of surveillance of their deliveries or taxi trips on the road. They should not accept it in the sky,” Wing argues.

With that kind of language, you might think Wing is arguing that drones shouldn’t broadcast their location, yes? Amusingly, no: the Alphabet subsidiary just wishes they’d send it through the internet instead of broadcasting it locally. I think my former *CNET* colleague Ian Sherr’s tweet is apt:

> *I am shocked — shocked — that a company being investigated for antitrust concerns over abusing its power on the internet would recommend the FAA ditch its newest radio-frequency ID program for internet-based tracking. https://t.co/d6VNMPapth*
>
> *— Ian Sherr (@iansherr) December 31, 2020*

Internet-based tracking is exactly what the FAA had originally intended to do when it first proposed the Remote ID rules back in December 2019, by the way — before it received a laundry list of reasons from commenters why internet-based tracking might be problematic and decided to abandon it. Here are just a few of the ones mentioned:

- The cost of adding a cellular modem to a drone to begin with
- The cost of paying for a monthly cellular data plan just to fly a drone
- The lack of reliable cellular coverage across the entirety of the US
- The cost of paying a third-party data broker to track and store that data
- The possibility of that third-party data broker getting breached
- The possibility of that data broker or network getting DDoS’d, grounding drones in the US

If you want to read the whole argument for yourself, the FAA

spends 15 pages laying out and contemplating all the objections to internet-based Remote ID in its full rule (PDF) starting at page 60.

Personally, I think it's pretty ridiculous that the FAA felt it had to choose between "everyone has to broadcast their location to everyone within earshot" and "everyone has to pay gobs of money to private industry and trust some data broker with their location," but the reasons why we aren't going with internet-based tracking make some sense to me.

Most proponents of Remote ID technology, including Wing, like to explain that it's merely a "license plate" for the skies, perhaps nothing more intrusive than you'd already have on your car. Here's Wing on that:

> *This allows a drone to be identified as it flies over without necessarily sharing that drone's complete flight path or flight history, and that information, which can be more sensitive, is not displayed to the public and only available to law enforcement if they have proper credentials and a reason to need that information.*

But the thing about license plates is, traditionally, you have to be within eyeshot to see them. You'd have to be physically following a car to track it. That's not necessarily true of a broadcasting transmitter, and it's potentially *far* less true of a internet-based solution like the one Wing seems to wish the FAA had offered instead. Naturally, it depends on who owns the internet-based solution and how much you trust them and their security.

Either way, it's going to be a while before we find out how secure or vulnerable, how broad or narrow these Remote ID broadcasts are truly going to be. That's because the FAA's final rule doesn't actually mandate what kind of broadcasting tech drones will be required to use: companies have the next year and half to figure that out, and they have to submit it

to the FAA for approval. The FAA is also clear that broadcast Remote ID is just a first step, an “initial framework,” suggesting that internet-based Remote ID might still be an option in the future.

https://www.theverge.com/2021/1/1/22209558/google-wing-faa-drone-remote-id-broadcast-rule-privacy-security