From: Margot E. Kaminski

Assistant Professor of Law

Moritz College of Law

The Ohio State University

To: The Honorable Tony Cárdenas

House of Representatives

Committee on Energy and Commerce

Re: The Disrupter Series: The Fast-Evolving Uses and Economic Impacts of Drones

1. **Would you agree that the largest companies have the greatest ability to acquire the most sophisticated unmanned aircraft and thus also to engage in the most far-reaching surveillance?**

Large companies are likely, depending on their business model, to pose significant threats to privacy. They will not necessarily, however, be the sole or even the main source of surveillance harms. A lot depends on business model, and the development of companies that aggregate information gathered by smaller drone operators.

Surveillance tends to causes harms in the following situations: when it is persistent (it follows a particular person around for a long period of time); when it is pervasive (it follows everyone, everywhere); when it is disruptive (the information gathered is used out of context); and when it

gathers sensitive information about a person. The largest companies are most likely to contribute to pervasive surveillance (following everyone, everywhere), depending on the scope and purpose of their operations. Large companies that have the goal of profiling particular individuals will also contribute to persistent surveillance. But even small companies and individuals can easily cause multiple kinds of surveillance harms. And small companies and individuals are likely in the aggregate to contribute to a pervasive surveillance environment, absent further regulation. One can imagine a business model that aggregates data gathered by individuals or smaller companies; that aggregation could be as harmful to privacy as actions by a larger company acting alone.

Larger companies arguably have greater incentives to self-regulate, since they are the biggest targets for regulators. A company that primarily wants to use drones to deliver packages, for example, does not want to be a visible privacy violator, for fear that Congress will enact legislation targeting its practices, or the FTC will pursue a Section 5 complaint. This is not to say that larger companies will effectively self-regulate; just that given their higher profiles, they are likely to avoid the most visibly egregious offenses.

2. **Could Congress condition authorization to fly on a pledge to respect privacy? For example if the FAA insists that before receiving permission to operate an unmanned aircraft, a business or individual first would have to commit to observing applicable privacy laws?**

This is a fascinating idea. Congress already conditions airman certificates (pilot licenses) on

compliance with federal airborne hunting laws.[1] If a pilot is convicted of violating section 13(a) of the Fish and Wildlife Act of 1956, the FAA may issue an order revoking his or her license.

There are four points worth considering, however. First, the FAA's expertise is largely concentrated on aircraft safety; it has explicitly disavowed involvement in privacy regulation concerning drones.[2] Imposing this requirement could have high costs for the FAA, both in monitoring for compliance and in developing agency expertise in this area, since presumably not every privacy violation would result in the revocation of a license.

Second, this model of requiring a business to make a privacy promise and enforcing compliance is largely the model of regulation pursued by the FTC (although there, the privacy promise usually extends beyond legal requirements). It would better comport with agency expertise to involve the FTC in a proposal like this.

Third, state laws may not adequately protect privacy, and are not consistent across states (which in fact can be one of their benefits—this allows for experimentation). While some states have enacted drone-specific legislation, many others have not, and older state privacy laws such as intrusion upon seclusion and Peeping Tom laws will not reach many of the types of privacy violations people fear from drones.[3] A citizen in one state could end up with far more protections than a citizen in another.

[1] 49 U.S.C. §44709(b)(2); 16 U.S.C. §742j-1(a).
[2] See letter dated November 26, 2014, dismissing EPIC's petition for rulemaking on the threat of privacy and civil liberties that will result from the deployment of aerial drones. https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf.
[3] Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 Cal. L.Rev. Cir. 57, 68 (2013).

Fourth, there may be First Amendment concerns raised by this proposal. Inasmuch as Congress wishes to keep the FAA away from First Amendment issues, it should keep this in mind. State privacy laws largely address the moment of recording information, and courts, as mentioned in my testimony, have begun explicitly recognizing a First Amendment right to record.

When a licensing regime involves speech, courts subject it to First Amendment scrutiny, asking whether it is narrowly drawn and restrictive of undue regulatory discretion.[4] Giving the FAA the discretion to revoke pilot licenses due to privacy violations might trigger these concerns—the more discretion an official has regarding hinging a licensed privilege on speech, the more likely a First Amendment licensing problem will be found. However, your model supposes that courts themselves will initially make the decision that there has been a privacy violation. This may help avoid a First Amendment problem, because presumably the courts themselves will consider the First Amendment when addressing the underlying privacy action.

3. **Would this give the FAA the discretion to rescind the operators' flight credentials, upon submission of proof that a court or similar body has faulted the operator for serious privacy violations under state law?**

Yes, Congress could structure FAA credentialing this way. However, see the concerns raised above. As long as the FAA licensing regime is restricted to legitimate safety issues, it will avoid First Amendment scrutiny. Adding privacy to the mix could subject FAA discretion to First

[4] See http://www.slate.com/articles/technology/future_tense/2014/11/faa_s_attempts_to_regulate_drones_could_have_first_amendment_problems.html.

Amendment analysis.

4. **Since violations occur under state law, this would mean that states would do the regulating. State regulators would do the litigating and state courts the adjudicating. The FAA would only get into the mix in extreme cases, correct?**

This would depend on how much discretion Congress gives to the FAA. The current regime for governing illegal airborne hunting permits but does not require the FAA to revoke a pilot's license.[5] If Congress gives the FAA similar discretion here, presumably the FAA would exercise that discretion and get involved only in extreme cases.

5. **Would this system of litigation be effective given that the violating companies with the most sophisticated unmanned aircrafts are best situated to withstand—injunctions, and money damages?**

More sophisticated companies would be less troubled by damages; that is correct. However, more sophisticated companies may be relatively good actors, given the potential that their actions will be highly visible, and fear of public backlash resulting in restrictive legislation. Drones face significant public acceptance hurdles, if state laws are any indicator. More sophisticated companies likely are aware of this. The worry is that this system would fail to deter smaller bad actors, whose cumulative impact on privacy could be huge. It would also fail to deter data privacy violations, as states do not regulate the reuse or misuse of data—just the initial gathering of it.

[5] 49 U.S.C. §44709(b)(2).

6. Would this proposal deter privacy violations—in advance of wholesale domestic drone integration, and in advance of long and uncertain litigation in state courts?

This proposal is intriguing. It could deter privacy violations by reminding companies that they are already subject to state privacy laws, and could make stickier companies' promises to respect privacy, by employing FAA enforcement on top of state enforcement.

My response to Question 2, above, raises some possible concerns with this proposal. An additional worry is that state laws do not address data privacy violations, so this proposal would have little impact on the reuse or misuse of data gathered by drones—hence my suggestion of technology-neutral federal data privacy law, enforceable by the FTC. Some have alternatively but similarly suggested requiring drone operators to submit a data privacy plan to the FAA, and allowing the FTC and state AGs to enforce the plan.[6]

Another point to keep in mind is that many drone users will not have traditional pilot's licenses—and thus may not feel the pain of having a license revoked. Model aircraft operators, for example, are not required to have a pilot's license;[7] and the FAA is contemplating creating a less stringent unmanned aircraft operator certificate with a small UAS rating for operation of drones weighing less than 55 pounds, and an even less stringent unmanned aircraft operator certificate with a micro UAS rating for operation of drones weighing less than 4.4 pounds.[8] The

[6] http://www.markey.senate.gov/imo/media/doc/2015-03-03-Drone_Legislation_Markey.pdf
[7] https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_91-57A.pdf.
[8] https://www.faa.gov/regulations_policies/rulemaking/media/021515_suas_summary.pdf; https://www.federalregister.gov/articles/2015/02/23/2015-03544/operation-and-certification-of-small-unmanned-

FAA is contemplating rules requiring only a signed statement to obtain the micro UAS operator certificate.[9]

If Congress decides to enforce privacy compliance through the FAA licensing process, it should be aware of these largely justified attempts to loosen aircraft operator certification requirements with respect to small drones. A privacy enforcement regime that operates on top of FAA certification would likely have the least impact on the actors using the smallest drones, for better or for worse.

Thank you for your questions, and again for the opportunity to testify. I hope these answers will be helpful to you.

Best,

Margot Kaminski

---

aircraft-systems#p-347; http://www.forbes.com/sites/gregorymcneal/2015/02/14/the-faa-may-get-drones-right-after-all-9-insights-into-forthcoming-regulations/

[9] https://www.federalregister.gov/articles/2015/02/23/2015-03544/operation-and-certification-of-small-unmanned-aircraft-systems#p-347 ("No knowledge test would be required in order to obtain an unmanned aircraft operator certificate with a micro UAS rating; instead, the applicant would simply submit a signed statement to the FAA stating that he or she has familiarized him or herself with all of the areas of knowledge that are tested on the initial aeronautical knowledge test that is proposed under part 107.")