NISKANEN CENTER

Public Interest Comment

Comments submitted to the Federal Trade Commission in the Matter of:

The Privacy Implications of Commercial Drone Operations

Ryan Hagemann
Technology and Civil Liberties Policy Analyst
The Niskanen Center

Submitted: November 13, 2016
Docket No. N/A (Subject Category: *Seminar Addressing Drones*)

Executive Summary

Unmanned aerial systems, or commercial drones, are the latest in a parade of emerging technologies capturing headlines. This technology has captured the public's imagination, leading many to consider the privacy ramifications of skies crowded with potential surveillance machines. The Federal Trade Commission is appropriately situated to deal with harms to consumers resulting from violations of privacy by operators of commercial drones. We acknowledge that problems may materialize in the future, but argue that there is no current justification for the agency to regulate this technology. In addition, we point to a number of existing authorities, best practices, and regulatory frameworks that can be applied to commercial drones without forestalling innovation and progress.

Introduction

The Niskanen Center concurs with the argument raised in the Federal Trade Commission's (FTC) call for comments, that: "While drones may offer numerous benefits, the potential for information collection raises the potential for consumer harms, including invasion of privacy, identification, trespass, and harassment."[1] However, it is also the case that "the potential for consumer harms" arising from "the potential for information collection" is not a concern unique to the operations of unmanned aerial systems (UAS), otherwise known as commercial drones. The key point we wish to emphasize is that the introduction of UASs to the national airspace does not constitute a particularly novel problem that would justify additional regulatory powers, or ex ante enforcement actions, from the FTC.

UAS Operations and Privacy Considerations

Defining privacy, or even particular propertied interests in the concept, is an unwieldy task. In general, the FTC has been able to make reasonably broad use of its discretionary Section 5 authority to police unfair and deceptive practices.[2] We would urge the agency to embrace regulatory restraint when assessing any potential role for expanded authorities over UAS-specific privacy considerations. This is especially important given ongoing innovation in this economically and socially transformative technology. If regulators give in to public fears over potential privacy concerns, onerous and prescriptive rules could very well forestall many benefits UASs have to offer. If these fears are unfounded—and history has shown they often are—restricting the use of the new technology will leave consumers worse off with no compensating benefit.

Daniel Castro, director of the Center for Data Innovation, appropriately sums up this perspective when commenting on recommendations from the White House report, "Big Data: Seizing Opportunities, Preserving Values." Despite reviewing "all of the harms from big data identified" in the report, he found:

> *that even though many commentators had expressed concern about big data, the report failed to identify almost any concrete examples of how big data is actually causing consumers economic, physical, or social harm. In fact, after reviewing all 37 concerns identified in the report, the Center found that all but two of them were purely speculative, i.e., the authors cited no evidence that the concerns mentioned were occurring today, and many were vague and ill-defined.*
>
> *This is a crucial point. If the White House had identified a broad series of tangible examples of how big data was presently harming consumers, then it would be*

[1] "Second of Three Seminars Addressing New and Evolving Technologies: Request For Public Comments," Federal Trade Commission, March 31, 2016, https://ftcpublic.commentworks.com/ftc/dronesseminar/.

[2] 15 U.S. Code § 45.

legitimately justified in calling for policymakers to adopt comprehensive consumer privacy rules. But since it did not, this raises the question of whether there is even a compelling need for policy intervention at this stage.[3]

Indeed, many technology policy scholars and analysts have echoed similar concerns over generalized privacy "threats" from new technologies.[4] Perhaps most importantly, embracing a more inflexibly precautionary regulatory framework for privacy (as it relates to data collection and usage issues) has been shown to be a death knell for innovation, investment, and economic growth.[5] Further, there is evidence of privacy regulations having a deleterious impact on competitive markets.[6] Most importantly, for the specific purpose of these comments, the Niskanen Center argues that there is nothing particularly novel or unique about UASs that would result in new, previously unimagined or unregulated privacy violations. As it happens, the FTC currently has a robust privacy framework that can adequately address potential consumer harms.

Where UAS-specific concerns do materialize, we believe the agency's current privacy framework will be sufficient to address any emergent problems.[7] Indeed, the framework points out that: "the

---

[3] Daniel Castro, Comments to the National Telecommunications and Information Administration, "Big Data and Consumer Privacy in the Internet Economy," Docket No. 140514424–4424–01, August 5, 2014, http://www2.datainnovation.org/2014-ntia-big-data.pdf.

[4] *See generally* Daniel Castro and Alan McQuinn, "The Privacy Panic Cycle: A Guide to Public Fears About New Technologies," Information Technology and Innovation Foundation, September 2015, http://www2.itif.org/2015-privacy-panic.pdf?_ga=1.80063124.2062395677.1439230224; *see also* Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology*, Vol. 14:1, http://conservancy.umn.edu/bitstream/handle/11299/144225/Technopanics-by-Adam-Thierer-MN-Journal-Law-Science-Tech-Issue-14-1.pdf;jsessionid=F62D9C5FBB29D914CA1D321632617051?sequence=1.

[5] Paul Hofheinz and Michael Mandel, "Bridging the Data Gap: How Digital Innovation Can Drive Growth and Create Jobs," The Lisbon Council/Progressive Policy Institute, Issue 15, 2014, http://www.progressivepolicy.org/wp-content/uploads/2014/04/LISBON_COUNCIL_PPI_Bridging_the_Data_Gap2.pdf, p. 14. ("To date, Europe lags far behind the US and Japan in terms of broadband adoption and investment—a worrisome trend on any day, but also a source of great opportunity in the future. Telco investment actually rose in the US and Japan in 2012, climbing 6.7% and 7.5%, respectively. But it was decidedly flat in Europe, where European providers, facing declining revenues brought on partly by their slowness in diversifying their services and embracing the big-data bandwagon, chose restraint.")

[6] Lucas Bergkamp, "The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy," *Computer Law & Security Report*, Vol. 18, no. 1, 2002, p. 39. ("A study by Kichenman established that: '[e]fforts to open the [EU] financial services industry—to foster the development of competition, better serve customers, lower prices, and compete more effectively with US institutions—have largely failed because of restrictive privacy laws.' Restrictive privacy laws act as a competition barrier by giving the dominant incumbent firm a monopoly over the customer information it possesses while denying new market entrants the information needed to offer and market financial services. As a result, Kitchenman concludes, consumer lending is not common and where it exists, it is concentrated among a few major banks in each country, each of which has its own large database.")

[7] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," Federal Trade Commission Report, March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. (Despite our general support for the framework, concerns linger that, as currently constructed, these "voluntary best practices" may end up being enforced through legislative statute. In particular, we agree with Commissioner J. Thomas Rosch's dissent: "Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson

Commission agrees that any privacy framework should be technology neutral."[8] Although specifically referencing internet service providers, this agreement should—and we would argue, does—extend to new emerging technology platforms like UASs. Other commentators have similarly agreed with respect to this interpretation.[9] A common theme running through that framework references lackluster willingness of industry groups to "promote enforceable self-regulatory codes." However, the FTC makes it clear that if such codes are developed, with respect to consumer data collection privacy best practices, it "will view adherence to such codes favorably."[10] With regards to data collection by UASs, such codes of conduct have already been developed.

To wit, the National Telecommunications and Information Administration (NTIA) recently released its consensus, stakeholder-drafted best practices covering UAS privacy, transparency, and accountability.[11] These best practices were developed by a broad multistakeholder community that involved members of civil society, industry, and government, among others. It is particularly noteworthy to point out that the guiding document does not "intend to discourage unplanned or innovative data uses that may result in desirable economic or societal benefits."[12] As a result, its impact on commercial UAS innovation could be largely beneficial, assuming the FTC and other regulatory bodies embrace regulatory forbearance.[13]

Policy Recommendations

Between the FTC's current privacy framework and NTIA's UAS best practices guidelines, an ample and robust body of documents already exist that can help guide privacy considerations related to UAS operations. These existing frameworks suffice to remedy any potential concerns associated with UAS operations. As such, the Niskanen Center argues that no further guidelines, regulatory authorities, or legislative action is currently necessary to address UAS-specific privacy issues.

---

that the recommendations of the final Report are supposed to be nothing more than 'best practices,' I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement. … [E]ither these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in which case there can be no pretense that they are 'voluntary.' It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the 'best practices' or face the wrath of 'the Commission' or its staff.")

[8] "Protecting Consumer Privacy in an Era of Rapid Change," p. 56.

[9] "In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," Comments of the International Center for Law & Economics and Scholars of Law & Economics, submitted to the Federal Communications Commission, WC Docket No. 16-106, May 27, 2016.

[10] "Protecting Consumer Privacy in an Era of Rapid Change," p. ix. ("To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.')

[11] "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability," May 18, 2016, https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

[12] "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability," p. 5.

[13] *See generally* Maureen K. Ohlhausen, "The FCC's Knowledge Problem: How to Protect Consumers Online," *Federal Communications Law Journal*, Issue 2, Vol. 67, https://www.ftc.gov/system/files/documents/public_statements/818521/1509fccohlhausen.pdf.

Additionally, the FTC is currently well-positioned to address issues related to consumer harm as they arise under its Section 5 authority. No further rules, regulations, or multistakeholder processes seem warranted unless or until new, non-trivial issues unique and specific to UAS operations emerge. Until such time as those issues are shown to warrant further action, the Niskanen Center recommends that the FTC take no further action on privacy or consumer harm issues related to UASs.

Conclusion

The privacy implications of commercial drone operations are not fundamentally different from those associated with other new emerging technologies. In addition to that simple fact, existing best practices, regulatory authorities, and state and local laws are more than adequate to deal with any potential harms that may arise. As such, the Niskanen Center argues that there is no further role for the FTC to play in addressing privacy issues related to UAS operations at this time. We commend the FTC taking the initiative in convening these workshops, and applaud its commitment to stakeholder inclusivity. However, we caution against the agency taking any action that could be viewed as a stalking horse of regulation or legislation down the road.

We thank the FTC for the opportunity to comment on these issues and look forward to an ongoing and productive dialogue on this issue.