



**Comments on the
Federal Trade Commission Fall Technology Series: Drones**

Submitted November 14, 2016



November 14, 2016

Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20530

Re: FTC Fall Technology Series: Drones

The Commercial Drone Alliance is grateful for the opportunity to comment on the drone workshop hosted by the Federal Trade Commission (“FTC” or “Commission”) on October 13, 2016.

I. About Us

The Commercial Drone Alliance is an industry-led, 501c6 non-profit association representing the commercial drone end user community. We advocate on behalf of our community for streamlined and advanced operations of drones and we educate to prove the value and benefit of drone technology for commercial use. Our members and partners cover the entire ecosystem of the drone market, including commercial end users, manufacturers, service providers, government agencies, associations and more. Our goal is to alleviate barriers to drone adoption including regulatory challenges, privacy concerns, and public perception issues.

The Federal Aviation Administration (“FAA”) estimates that by 2020 there will be 11 million commercial drones sold in the United States¹ as commercial enterprises discover the value and benefit drone technology. However, widespread deployment of drones also poses certain safety, privacy and security challenges that will require collaboration between industry and government to ensure the successful integration of Unmanned Air Systems (“UAS”) into the national airspace.

The strategy of the Commercial Drone Alliance is to achieve rapid commercial integration of drones by working closely with federal, state and local governments and the broader UAS stakeholder community. We educate policymakers and influencers about drone user needs, demonstrate the safety and reliability of drone technology, and provide guidance on appropriate policy and legislation to more broadly authorize the commercial use of drones. We work with government agencies to move policy forward on issues such as safety, privacy, spectrum, cyber security, and more.

To this end, the Commercial Drone Alliance participated in the National Telecommunications and Information Administration (“NTIA”) process to help create privacy best practices for

¹ *Registration and Marking Requirements for Small Unmanned Aircraft*, 80 Fed. Reg. 78,594, 78,598 (Dec. 16, 2015) (interim final rule), <https://www.gpo.gov/fdsys/pkg/FR-2015-12-16/pdf/2015-31750.pdf>.



adoption by the drone community. In 2015 and 2016, this multi-stakeholder group of industry representatives, privacy advocates, and academics engaged in lengthy, robust dialogue to craft the appropriate guidance for protecting privacy and data security during routine commercial drone operations. The NTIA process resulted in a meaningful document that is supported by leaders in the drone industry, including the Commercial Drone Alliance on behalf of its members.

Our Alliance is pleased to offer comments to the FTC as it begins to educate itself on the drone industry and the many standards, laws, and common law rights that already provide meaningful privacy and data protections for consumers. We believe that further guidance or regulation by the FTC at this time would not be in keeping with the Commission's careful approach to the regulation of new technologies or its history of developing technology-neutral standards.

II. Drones will be a Driver for Economic Growth and Innovation with a Supportive and Thoughtful Regulatory System

UAS is an Emerging, Dynamic Industry

Commercial drones have captured the imagination of entrepreneurs, innovators, public agencies, and policymakers across the country. From disaster response to farming to newsgathering to infrastructure inspection and more, drones provide a safer and more efficient alternative to manned flights, enhancing American productivity in a multitude of ways. Over time, we know that the economic benefits of the drone market will be significant. Expert estimates vary, but the numbers are all large. A recent PricewaterhouseCoopers report estimates the global market value of drone-powered solutions at over \$127 billion.² In the United States, over the next decade and assuming the regulatory framework keeps pace, the domestic drone industry is projected to grow into an \$82 billion market while creating more than 100,000 new jobs.³ And, by 2020—less than four years from now—there will be 11 million commercial drones sold in the United States alone.⁴

Given the many benefits of this technology, the broad integration of commercial UAS into the National Airspace represents an exceedingly exciting opportunity. But innovation does not happen in a vacuum; we need to ensure policy supports and enables this growth.

² Michal Mazur et al., *Clarity From Above: PwC Global Report on the Commercial Applications of Drone Technology* 1 (May 2016), <http://www.pwc.pl/pl/pdf/clarity-from-above-pwc.pdf>. (This number represents the “value of current business services and labour that have a high potential for replacement in the very near future by drone powered solutions.”).

³ The White House, *FACT SHEET: New Commitments to Accelerate the Safe Integration of Unmanned Aircraft Systems* (Aug. 2, 2016), <https://www.whitehouse.gov/the-press-office/2016/08/02/fact-sheet-new-commitments-accelerate-safe-integration-unmanned-aircraft>.

⁴ Fed. Reg. at 78,598.



The United States has a History of Being Careful not to Over-Regulate Emerging Technology

The United States historically refrains from over-regulating emerging technologies. The commercial development of the Internet is but one example. The Internet economy grew rapidly in the United States due in part to a carefully crafted regulatory system that encouraged innovation. In its 1997 “Framework for Global Electronic Commerce,” the Clinton administration stated that “[t]he private sector should lead [and] [t]he Internet should develop as a market driven arena not a regulated industry.”⁵ The Clinton administration also argued that “governments should encourage industry self-regulation and private sector leadership where possible” and “avoid undue restrictions on electronic commerce.”⁶

In recent years, FTC leadership has cited the successful regulatory scheme that supported the growth of the Internet as a model for regulation of new technologies. FTC Commissioner Ohlhausen has said, “The success of the Internet has in large part been driven by the freedom to experiment with different business models, the best of which have survived and thrived, even in the face of initial unfamiliarity and unease about the impact on consumers and competitors.”⁷ “It is . . . vital that government officials, like myself, approach new technologies with a dose of regulatory humility, by working hard to educate ourselves and others about the innovation, understand its effects on consumers and the marketplace, identify benefits and likely harms, and, if harms do arise, consider whether existing laws and regulations are sufficient to address them, before assuming that new rules are required.”⁸

Echoing this sentiment, the FTC’s 2015 staff report on the Internet of Things (“IoT”) acknowledged that IoT is in its early stages and recognized that specific new rules would be premature. The report stated, “[t]he Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a

⁵ The White House, *The Framework for Global Electronic Commerce: Executive Summary*, <https://clinton4.nara.gov/WH/New/Commerce/summary.html> (last visited Nov. 14, 2016).

⁶ *Id.*

⁷ Maureen K. Ohlhausen, Comm’r, Address at the FTC Internet of Things Workshop: *The Internet of Things: When Things Talk Among Themselves* 1 (Nov. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-commissioner-maureen-k.ohlhausen-ftc-internet-things-workshop/131119iotspeech.pdf.

⁸ *Id.*



means to encourage the adoption of privacy- and security-sensitive practices.”⁹ The FTC also deliberately used language in its IoT report that did not mandate any particular data security action by IoT companies. Specifically, the FTC’s report stated that companies “should consider” certain practices rather than requiring that these practices be carried out. FTC staff also acknowledged that certain privacy safeguards, such as data minimization, are “challenging” in the context of IoT and recommended that the industry determine for itself reasonable limits on the collection and retention of consumer data.¹⁰

Holistic, Technology-Neutral Approaches Should Remain a Hallmark of the FTC

The FTC’s privacy and data security guidance and standards take a holistic, technology-neutral approach. As early as 1998, the Commission published a report on online privacy that applied generally to all sectors. The Commission reviewed hundreds of websites and did not confine itself to the collection of data from particular industries or only certain websites that collect a specific type of data, for instance, health data or financial data.¹¹ Since then, the FTC has continued to study the issues of privacy and data security through surveys, research and public comments, conferences, and workshops from a broad perspective.

Recently, the Commission published two technology neutral reports on consumer privacy and data security—*Protecting Consumers in an Era of Rapid Change*¹² and *Internet of Things: Privacy & Security in a Connected World*¹³—as well as a guidance document specifically addressing data security—*Start with Security: A Guide for Business*.¹⁴ One theme that is constant in these efforts is that the FTC is focused on the behavior of the actor and not the

⁹ FTC, *Internet of Things: Privacy & Security in a Connected World* 48-49 (Jan. 2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (footnote omitted).

¹⁰ *Id.*

¹¹ FTC, *Privacy Online: A Report to Congress* 21 (June 1998), <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf> (“The Comprehensive Sample (Sample A) includes 674 Web sites, and the types of companies included range broadly across the entire spectrum of the American economy.”).

¹² FTC, *Protecting Consumers in an Era of Rapid Change: Recommendations for Business and Policymakers* (Mar. 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

¹³ *See, supra* note 9.

¹⁴ FTC, *Start With Security: A Guide for Business* (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.



technology. We think this approach makes sense for the FTC’s consideration of drones, which is simply another one of the many IoT technologies. If the FTC decided to change its approach to produce guidance for each new IoT technology, it would lose the perspective that has guided its approach to consumer privacy and data security for almost two decades.

III. New Privacy or Data Security Guidance by the FTC Likely will Conflict with or Duplicate the NTIA Consensus Best Practices for Drones

To the extent that the FTC believes increased adoption of drone privacy and data security practices are needed, the Commission should encourage the voluntary adoption of the Best Practices published as part of the NTIA multi-stakeholder process.¹⁵

The NTIA multi-stakeholder process was launched by the White House in 2015 when it issued a Presidential Memorandum directing the NTIA to facilitate the creation of best practices for privacy, transparency, and accountability related to the private and commercial use of drones.¹⁶ Following the Presidential Memorandum, over the course of approximately nine months, industry representatives, privacy advocates and academics met to discuss drone privacy and data security standards. The multi-stakeholder group met as a whole many times for several hours each session and, in parallel, stakeholders and subgroups met numerous times, frequently on a daily basis. There was also much work done behind the scenes to consider the issues and how to reach consensus. Anyone interested in these issues was invited and encouraged to participate, and indeed participation in the process was robust from all sides.

The result of this hard work was a consensus set of privacy and data security Best Practices reached by a diverse group of stakeholders. The Best Practices encourage drone operators to:

- provide notice of use of drones operations and data handling practices;
- avoid the collection of data when the drone operator knows the data subject has a reasonable expectation of privacy;
- avoid the persistent and continuous collection of data on individuals without a compelling need to do so or consent;

¹⁵ *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability* (May 2016), https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

¹⁶ Press Release, The White House, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Feb. 2015), <https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua>.



- minimize the operation of drones over private property without legal authority or consent;
- avoid publicly disclosing personal information captured by drones when it is not necessary to fulfill the stated purpose for which the UAS is used; and
- manage security risks by implementing reasonable administrative, technical and physical safeguards to protect personal information collected by drones.

The Best Practices also provide important protections to safeguard the First Amendment rights of journalists and newsgatherers using drones. In sum, the Best Practices provide the emerging drone industry the room it needs to grow while also providing baseline privacy protections that can complement existing state, common law, and federal rules on the operation of drones. The Best Practices have been recognized by the Department of Commerce as “an important step in building consumer trust, giving users the tools to innovate in this space in a manner that respects privacy, and providing accountability and transparency.”¹⁷ And the White House encourages “all drone operators and companies to review the best practices and to determine whether and how to apply the practices to their own unmanned aircraft operations.”¹⁸ In conjunction with the White House’s Drone Innovation event this summer, the Commercial Drone Alliance and other industry groups committed to educate the public, including the drone industry at large, about the Best Practices.

Should the FTC believe that additional guidance is necessary for UAS operators, it should look no further than the Best Practices, which already provide a roadmap for action. We must give this process time to work.

IV. Existing State laws, Common Law Standards, and FAA Rules Provide Robust Privacy and Data Security Safeguards

State and Local Laws Protect Privacy and Data Security

In the United States, almost all States have general consumer protection laws that prohibit unfair or deceptive acts or practices, the enforcement of which could include drone activities that violate a person’s privacy or data security expectations. These rules mirror the FTC’s own authority over unfair and deceptive practices.

¹⁷ Angela Simpson, Deputy Assistant Sec’y for Commc’ns, & Info., NTIA, *Finding Common Ground on UAS* (May 2016), <https://www.ntia.doc.gov/blog/2016/finding-common-ground-uas>.

¹⁸ Press Release, The White House, *FACT SHEET, Enabling a New Generation of Aviation Technology*, (June 2016), <https://www.whitehouse.gov/the-press-office/2016/06/21/fact-sheet-enabling-new-generation-aviation-technology>.



In addition, rules regarding property rights and privacy in the context of drone operations have been adopted at the state and local level. At least ten States, including Arkansas, Florida, Idaho, Indiana, Louisiana, North Carolina, Oregon, Tennessee, Texas, and Wisconsin, and cities such as Chicago and Los Angeles, already have enacted privacy laws that regulate the commercial and private use of drones. These state laws take many different forms. Idaho’s law specifically prohibits drones from photographing or recording an individual for purposes of publicly disseminating the information without the individual’s written consent.¹⁹ Other laws prohibit the use of drones to record or survey private property. Louisiana’s drone law, for instance, prohibits the use of drones to conduct surveillance of certain manufacturing facilities.²⁰ States also have privacy laws that do not explicitly mention drones, but are broad enough to cover drone activities. California’s law, for instance, prohibits the capture of images taken in an offensive manner of an individual engaging in a personal or familial activity.²¹ States also have rules against peeping Toms, and individuals can bring nuisance claims and suits against trespassers related to drones.

At least eleven States—Arkansas, California, Connecticut, Florida, Maryland, Massachusetts, Nevada, Oregon, Rhode Island, Texas, and Utah—impose various levels of data security requirements that could apply to drone use.²² While there are some variations, these laws generally require that businesses implement and maintain “reasonable” procedures to safeguard personal information.²³ The most detailed and comprehensive of the state information security laws is the Standards for the Protection of Personal Information of Residents of the

¹⁹ Idaho Code Ann. § 21-213.

²⁰ La. Stat. Ann. § 14:337.

²¹ Cal. Civ. Code § 1708.8(b), (l)(1)(A) (“A person is liable for constructive invasion of privacy when the person attempts to capture, in a manner that is offensive to a reasonable person, any type of visual image, sound recording, or other physical impression of the plaintiff engaging in a private, personal, or familial activity” “under circumstances in which the plaintiff had a reasonable expectation of privacy,” “through the use of any device, regardless of whether there is a physical trespass, if this image, sound recording, or other physical impression could not have been achieved without a trespass unless the device was used.”).

²² Ark. Code Ann. § 4-110-104(b); Cal. Civ. Code § 1798.81.5; Conn. Gen. Stat. Ann. § 42-471; Fla. Stat. § 501.171(2); Md. Code Ann., Com. Law § 14-3503; Nev. Rev. Stat. Ann., Ch. 603A; Or. Rev. Stat. Ann. § 646A.622; 11 R.I. Gen. Laws Ann. § 11-49.3-3; Tex. Bus. & Com. Code Ann. § 521.052; Utah Code Ann. § 13-44-201.

²³ See e.g., Tex. Bus. & Com. Code Ann. §521.052(a).



Commonwealth of Massachusetts, (“Massachusetts Standards”).²⁴ The Massachusetts Standards apply to all businesses (including potentially drone operators) that receive, store, maintain, process, or otherwise have access to “personal information” about a resident of Massachusetts in connection with the provision of goods or services or in connection with employment.²⁵ The Massachusetts Standards include approximately thirty discrete obligations concerning administrative, physical, and technical safeguards that organizations are expected to satisfy when handling the sensitive personal information of Massachusetts residents. Covered businesses must develop, implement and maintain a comprehensive written information security program addressing the required safeguards. Other of the requirements include, as relevant to covered personal information, having an employee in charge of overseeing the security program, ongoing assessment and evaluation of risks, training and ensuring compliance with policies and procedures, oversight of third party service providers, and various computer security measures such as authentication, system access controls, encryption of files traveling across public networks and data held on laptops and portable devices.²⁶

Common Law Privacy Standards Protect Individuals’ Privacy

In addition to statutory and regulatory restrictions, there are common law privacy rules that may protect against certain misuse of drones. A person is subject to liability for the tort of intrusion upon seclusion if the person “intentionally intrudes...upon the solitude or seclusion of another or his private affairs or concerns...if the intrusion would be highly offensive to a reasonable person.”²⁷ In the context of drones, an individual could claim that aerial images of his or her property captured private details and intruded on his or her seclusion.

Property rights also may impact the use of drones. For instance, an intrusion into the airspace above the land of another can amount to a trespass. Under the Restatement of Torts, flights constitute a trespass if the aircraft “(a) enters into the immediate reaches of the airspace next to the land, and (b) it interferes substantially with the other’s use and enjoyment of the land.”²⁸

²⁴ 201 CMR 17.00; *see also* Office of Consumer Affairs & Bus. Regulation, *Frequently Asked Questions Regarding 201 CMR 17.00 (“FAQ”)*, <http://www.mass.gov/ocabr/docs/idtheft/201cmr17faqs.pdf> (last visited Nov. 14, 2016).

²⁵ 201 CMR 17.01(2), 17.02, 17.03. “Personal information” is defined as a “Massachusetts resident’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver’s license number or state-issued identification card number; or (c) financial account number, or credit or debit card number.” Pursuant to the statute, “[e]very person that owns or licenses personal information about a resident of the Commonwealth” must comply with the standard.

²⁶ *See FAQ, supra* note 24.

²⁷ Restatement (Second) of Torts § 652B (Am. Law Inst. 1977).

²⁸ *Id.* § 159 (Am. Law Inst. 1965).



Relatedly, a property owner can invoke nuisance doctrine to prohibit unwanted use of drones on her property. A private nuisance is an “invasion of another’s interest in the private use and enjoyment of land.”²⁹ A plaintiff could argue that the use of UAS interferes with his or her normal occupancy of the land by creating noise or flying low enough to create a safety or privacy risk.

The FAA’s Current Rules Impact Privacy

Although the FAA has stated it does not have privacy authority, and while the agency did not seek to regulate privacy in Title 14 of the Code of Federal Regulations Part 107, it is notable that the agency’s new safety rule impacts privacy. We provide below three examples of how Part 107 provides meaningful privacy implications.

Flights Over People. First, according to the FAA rule, drones may not operate over persons not directly participating in the drone flight, except when those persons are under a covered structure, inside a covered stationary vehicle, or when the FAA grants a specific waiver. This prohibition of flights over non-participating persons likely will result in generally limiting drone operations to unpopulated or sparsely populated areas or over tightly controlled private property.

Visual Line of Sight. Second, drones are required by the rule to remain within the visual line-of-sight of the pilot-in-command or the drone’s visual observer. The aircraft must remain close enough so those persons are capable of seeing the aircraft with vision unaided by any device other than corrective lenses. Although this rule aims to promote safety by limiting drone operations to a relatively confined space and ensuring constant visual contact between the pilot or visual observer and the aircraft, it also promotes privacy by precluding drone operators from observing distant subjects or places.

Night Operations. Third, the rule generally prohibits drone operations at night without a special waiver. Daylight-only operations or twilight operations—thirty minutes before official sunrise or thirty minutes after official sunset—with appropriate anti-collision lighting are allowed. Like the line of sight rule, the general prohibition on night operations has a key safety purpose of preventing flights at a time when reduced visibility increases the likelihood of collisions, but the rule also limits the ability to misuse drones to surreptitiously capture images under cover of darkness.

These requirements in the FAA’s new rule have clear privacy implications that provide a certain level of protection from the use of drones for invasive purposes. Over time, these standards may change as the industry grows and safety implications are addressed. In parallel with these efforts, new companies may look to adopt the NTIA privacy Best Practices or other voluntary standards that address privacy in this changing landscape.

²⁹ *Id.* § 821D (Am. Law Inst. 1979).



V. Conclusion

The U.S. drone industry is dynamic, emerging, and ready to grow. By all accounts, the industry has tremendous potential to create jobs, provide efficiencies, and improve safety. Given this potential, and the FTC's usual careful attention to new technology and promotion of technology-neutral standards, and the numerous local, state, and federal laws and common law standards that already regulate drone privacy and data security, we believe that further regulation or guidance by the FTC specific to drones is unwarranted and unnecessary. If the FTC believes that increased adoption of drone privacy and data security practices are needed, the Commission should encourage the voluntary adoption of the NTIA Best Practices, which have been lauded by the Department of Commerce, have the support of the White House, and are promoted by leaders in industry and the privacy advocacy community.