epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL AVIATION ADMINISTRATION

Safe and Secure Operations of Small Unmanned Aircraft Systems

[Docket No.: FAA-2018-1086; Notice No. 18-08]

April 15, 2018

By notice published February 13, 2019, the Federal Aviation Administration ("FAA") issued an advance notice of proposed rulemaking asking whether the FAA should promulgate new rulemaking to require security design measures and additional information disclosure to reduce public safety and national security concerns associated with the integration of unmanned aircraft systems ("UAS" or "drones") into the National Airspace System ("NAS").[1]

EPIC submits these comments to the FAA to recommend that the agency establish standards requiring (1) secure connection between drones and drone operators; (2) security safeguards for surveillance technology onboard drones; (3) adequate data security and privacy safeguards for collected data; and (4) remote identification and broadcasting of information about a drone's flight plans, intended use, and surveillance capabilities.

[1] Safe and Secure Operations of Small Unmanned Aircraft Systems, 84 Fed. Reg. 3732–39 (2019), https://www.federalregister.gov/documents/2019/02/13/2019-00758/safe-and-secure-operations-of-small-unmanned-aircraft-systems.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[2] For well over a decade, EPIC has maintained expertise on privacy, safety, and security concerns related to drones and has prominently advocated for better regulation of the national airspace related to these threats.[3] In 2012, EPIC, joined by more than one hundred experts and organizations, petitioned the FAA to undertake a rulemaking to establish privacy regulations prior to the deployment of commercial drones in the national airspace. In the Petition, EPIC described the many ways in which the deployment of drones would threaten important privacy interests.[4]

EPIC has long raised concerns about the risks associated with the hacking of drones. EPIC has testified before the Homeland Security Committee about these risks and has submitted comments to the FAA noting that "hackers can exploit weaknesses in drone software to gain control of a drone's movement and other features."[5] In EPIC's earliest comments to the FAA regarding drones, EPIC warned that "drone hacking can expose troves of sensitive data" and "poses a threat to the security of lawful drone operations."[6]

[2] EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones* (2019), https://epic.org/privacy/drones; EPIC, *Spotlight on Surveillance: Unmanned Planes Offer New Opportunities for Clandestine Government Tracking* (Aug. 2005), https://epic.org/privacy/surveillance/spotlight/0805.
[4] Petition from EPIC et al., to Michael P. Huerta, Acting Adm'r, Fed. Aviation Admin. (Mar. 8, 2012), *available at* https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.
[5] *Using Unmanned Aerial Systems Within the Homeland: Security Game-Changer?: Hearing Before the Subcomm. on Oversight, Investigations, & Mgmt. of the H. Comm. on Homeland Sec.*, 112th Cong. 49 (2012) (statement of Amie Stepanovich, Ass'n Litig. Counsel, EPIC), *available at* https://www.govinfo.gov/content/pkg/CHRG-112hhrg80848/pdf/CHRG-112hhrg80848.pdf [hereinafter *UAS Within the Homeland Hearing*]; EPIC, Comments on the *Operation and Certification of Small Unmanned Aircraft Systems*, Fed. Aviation Admin. Docket No. FAA-2015-0150, at 5 (Apr. 24, 2015), https://epic.org/privacy/litigation/apa/faa/drones/EPIC-FAA-NPRM.pdf [hereinafter EPIC Comments on Operation & Certification of sUAS].
[6] EPIC, Comments on *Unmanned Aircraft System Test Sites*, Fed. Aviation Admin. Docket No. FAA—2012— 0252, at 6 (May 8, 2012), https://epic.org/apa/comments/EPIC-Drones-Comments-2012.pdf.

EPIC has repeatedly submitted comments to the FAA recommending that drone registration include disclosure of surveillance capabilities and explaining the necessity of active broadcast of registration information.[7] In earlier comments, EPIC stated "[t]he widespread deployment of drones in the United States is one of the greatest privacy challenges facing the Nation."[8] EPIC also testified to legislative bodies on the "unique threat to privacy" posed by drones[9] because "[t]he technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology."[10]

EPIC has specifically recommended that drones broadcast location, course, and purpose.[11] EPIC wrote earlier that:

> passive registration does nothing to address the privacy risks posed by drones in the national airspace, which undermines the safe integration of drones into the national airspace. Drones should be required to broadcast their registration information to allow members of the public and law enforcement officials to easily identify the operator and responsible party.[12]

EPIC also wrote at the time:

> Because drones present substantial privacy and safety risks, EPIC recommends that any drone operating in the national airspace system include a mandatory GPS

[7] EPIC, *Comments of the Electronic Privacy Information Center to the Federal Aviation Administration of the Department of Transportation Docket No. FAA-2013-0061: Unmanned Aircraft System Test Site Program* 10 (Apr. 23, 2013), https://epic.org/apa/comments/EPIC-Drones-Comments-2013.pdf; EPIC, Comments on the *Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) and Request for Information Regarding Electronic Registration for UAS*, Fed. Aviation Admin. Docket No. FAA-2015-4378, at 9–11 (Nov. 12, 2015), https://epic.org/privacy/drones/EPIC-FAA-Drone-Reg-Comments.pdf [hereinafter EPIC Comments on Clarification of Registration Requirements].

[8] EPIC Comments on Operation & Certification of UAS, *supra* note 5, at 5.

[9] *Use of Unmanned Aerial Vehicles (Drones): Hearing Before the S. Majority Policy Comm. of the Gen. Assemb. of Pa.*, 1–2 (2016) (statement of Jeramie D. Scott, Nat'l Sec. Counsel, EPIC), https://epic.org/privacy/drones/EPIC-Drone-Testimony-20160315.pdf; *Crimes – Unmanned Aircraft Systems – Unauthorized Surveillance: Hearing Before the H. Judiciary Comm. of the Gen. Assemb. of Md.*, 435th Sess. 1–2 (2015) (statement of Jeramie D. Scott, Nat'l Sec. Counsel, EPIC), https://epic.org/privacy/testimony/EPIC- Statement-House-Bill-620.pdf [hereinafter *UAS Unauthorized Surveillance Hearing*]; *UAS Within the Homeland Hearing*, *supra* note 5, at 4.

[10] *UAS Unauthorized Surveillance Hearing*, *supra* note 9, at 1 (statement of Jeramie D. Scott, Nat'l Sec. Counsel, EPIC).

[11] EPIC Comments on Clarification of Registration Requirements, *supra* note 7, at 4.

[12] *Id.* at 11.

> tracking feature that would always broadcast the location of a drone when aloft (latitude, longitude, and altitude), course, speed over ground, as well as owner identifying information and contact information.[13]

I. The FAA Must Establish Security Standards to Prevent the Hacking of Drones

EPIC supports the FAA's advance notice of proposed rulemaking and invitation for public comments on ways to ensure the safe integration of drones into the National Airspace. The FAA has acknowledged that an operator can lose positive control of a drone when there is system failure or when the operator flies the drone "beyond the signal range or in an area where control link communication between the aircraft and the control station is interrupted."[14] However, the FAA must recognize that hackers not only can cause an operator to lose positive control, but they can also commandeer the maneuverability and surveillance capabilities of drones, raising significant safety and privacy concerns. Therefore, the FAA—an agency "provid[ing] the safest, most efficient aerospace system in the world"[15]—must establish security design standards requiring a secure connection between drone operators and drones to protect operator control and collected data.

The vulnerability of drones to hacking is indisputable. Drones, like other electronic devices, are exposed to many cybersecurity threats.[16] Both the public and private sectors have acknowledged that the same GPS system and computers onboard a drone that enable its remote control through a communication channel are also its greatest vulnerability for cyberattacks.[17] In

[13] *Id.*
[14] Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9,544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, and 183).
[15] FAA, *Mission*, https://www.faa.gov/about/mission (last visited Apr. 12, 2019).
[16] Pierluigi Paganini, *Hacking Drones . . . Overview of the Main Threat*, Infosec Inst. (June 24, 2013), http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats.
[17] Aerospace Eng'g & Eng'g Mechs., Univ. of Tex., *Todd Humphreys' Radionavigation Lab Demonstrates First Successful 'Spoofing' of UAVs*, (July 12, 2012), http://wncg.org/news/todd-humphreys-radionavigation-lab-demonstrates-first-successful-spoofing-uavs; Kacey Deamer, *How Can Drones Be Hacked? Let Us Count the Ways*, Live Sci. (June 10, 2016),

2012, researchers at the University of Texas successfully commandeered a hovering drone from more than a half-mile away using a $1,000 device.[18] The researchers used a technique called "spoofing"—sending fake GPS signals that trick a drone's receiver as to the drone's location and the time and exploiting that "civilian GPS signals . . . are unencrypted and unauthenticated."[19] This research demonstrated that hacking drones is both possible and inexpensive.[20]

Researchers have also hacked and caused drones to crash using other methods, such as exploiting Wi-Fi vulnerabilities or overloading a drone's processing capacity.[21] Moreover, drone-specific vulnerabilities are delineated online and guides explaining how to hack drones have become publicly available, enabling even a novice to hack and gain control of a drone

http://www.livescience.com/55046-how-can-drones-be-hacked.html; *see* John A. Volpe, Nat'l Transp. Systems Ctr., Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System 57 (2001), https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf (acknowledging that GPS is a "tempting target that could be exploited" by jamming GPS service or "inducing a GPS receiver to produce misleading information").

[18] Robert N. Charette, *Drones and GPS Spoofing Redux*, IEEE Spectrum (July 6, 2012), https://spectrum.ieee.org/riskfactor/aerospace/aviation/-drones-and-gps-spoofing-redux.

[19] Daniel P. Shepard et al., *Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle*, GPS World, August 2012, at 30–31, https://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf; Charette, *supra* note 18 (quoting Todd Humphreys, Dir., Radionavigation Lab., Univ. of Tex.); *see* Paganini, *supra* note 16 (explaining that spoofing enables a hacker to "spoon feed" a drone false navigation information).

[20] *See* Charette, *supra* note 18 (hacking a drone with equipment worth approximately $1,000); *see also* Jill Scharr, *How to Hack Other People's Drones for Less than $400*, Tom's Guide (Dec. 4, 2013), https://www.tomsguide.com/us/skyjack-hacks-drones,news-17943.html (instructing how to hack a drone for approximately $400).

[21] April Glaser, *The U.S. Government Showed Just How Easy It Is to Hack Drones Made by Parrot, DBPower and Cheerson*, Recode (Jan. 4, 2017), https://www.recode.net/2017/1/4/14062654/drones-hacking-security-ftc-parrot-dbpower-cheerson (explaining how researchers from the Federal Trade Commission commandeered the maneuverability of two drones by exploiting the drones' unencrypted and non-password protected Wi-Fi signals); Phil Sneiderman-Jhu, *Here's How Easy It Is to Hack a Drone and Crash It*, Futurity (June 8, 2016), https://www.futurity.org/drones-hackers-security-1179402-2 (identifying three methods to crash a drone: overloading a drone's central processing unit with wireless connection requests, sending a data packet exceeding the capacity of a buffer in the drone's flight application, and sending fake signals to the drone's controller to make the controller believe a different device is the drone and, consequently, severing the controller's connection with the real drone).

midflight.[22] Absent secure connection standards, hackers can exploit the cybersecurity vulnerabilities of drones to commandeer and to transform drones into "potential missile[s]."[23]

EPIC advocates that "[t]he safe operation of drones depends on the implementation of cyber security measures to prevent drones from being hacked."[24] And EPIC recommends that the FAA "establish minimum security standards to prevent the loss of positive control" and encourages the FAA to promulgate minimum security standards to protect against the risks of drone hacking.[25]

One such minimum security standard should require encryption and authentication of GPS signals and Wi-Fi access points. Researchers agree that encryption and authentication can mitigate or prevent drones from being hacked. Dr. Todd E. Humphreys, the University of Texas researcher who spearheaded the first hacking of a civilian drone in 2012, has long called for these safeguards:

> Further research into cryptographic authentication methods should also be pursued. Officials in the U.S. Department of Transportation, the Federal Aviation Administration, and the Department of Homeland Security should be persuaded to

[22] Dan Goodin, *Flying Hacker Contraption Hunts Other Drones, Turns Them into Zombies*, Arstechnica (Dec. 3, 2015), https://arstechnica.com/information-technology/2013/12/flying-hacker-contraption-hunts-other-drones-turns-them-into-zombies (describing the release of specifications to "build an aerial drone that seeks out other drones in the air, hacks them, and turns them into a conscripted army of unmanned vehicles under the attacker's control"); Sander Walters, *How Can Drones Be Hacked? The Updated List of Vulnerable Drones & Attack Tools*, Medium (Oct. 29, 2016), https://medium.com/@swalters/how-can-drones-be-hacked-the-updated-list-of-vulnerable-drones-attack-tools-dd2e006d6809; *Which Is More Dangerous, Drone Hacking or Unsafe Drone Operation?*, DIY Drones (Dec. 26, 2013), https://diydrones.com/profiles/blogs/which-is-more-dangerous-drone-hacking-or-unsafe-drone-operation (explaining how Wi-Fi linked drone controls can be easily hacked).

[23] *See* Oliver Wyman, *Why the Use of Drones Still Faces Big Regulatory Hurdles*, Forbes (Sept. 10, 2018), https://www.forbes.com/sites/oliverwyman/2018/09/10/why-the-use-of-drones-still-faces-big-regulatory-hurdles/#3a7956be1c0d (noting that drones can be hacked for cyber terrorism and recommending that the FAA require the incorporation of IT security and redundancy safeguards).

[24] *See* EPIC Comments on Operation & Certification of sUAS, *supra* note 5, at 13; *see also* Evan Carr, Nat'l Ctr. for Policy Analysis, Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace 20 (2013), *available at* http://www.ncpathinktank.org/pdfs/sp-Drones-long-paper.pdf ("If UASs are easily manipulated by outsiders, the consequences could be grave.").

[25] EPIC Comments on Operation & Certification of sUAS, *supra* note 5, at 16.

> consider the perils of civil GPS spoofing and to oversee development and adoption of effective countermeasures.[26]

Researchers from the FTC have advised that "[d]rone manufacturers can . . . make their drones more secure by encrypting the Wi-Fi signal and adding password protection."[27] Others have recognized encryption as one of the integral safeguards to maximize drone security and to prevent loss of positive control:

> The best [UAS] communication to use is one that not only has a private network, but one that offers several layers of encryption, such as a proprietary encryption mechanism in addition to the option for the user to add his or her own unique encryption key.[28]

Despite prior concerns about the practical and economic feasibility of encrypting drone communication channels,[29] technological advancements have led to cheaper and more energy efficient cryptographic algorithms to implement in drones.[30] In fact, at least one civilian drone manufacturer has already implemented these safeguards.[31]

[26] Todd E. Humphreys et al., Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer 12 (2008), *available at* https://gps.mae.cornell.edu/humphreys_etal_iongnss2008.pdf.

[27] Glaser, *supra* note 21.

[28] *Choosing the Right UAS Data Link to Ensure Your Drone Remains Secure*, SkyHopper (Aug. 31, 2017), http://www.skyhopper.biz/drone-security.

[29] *See, e.g.*, Andy Greenberg, *Hacker Says He Can Hijack a $35k Police Drone a Mile Away*, Wired (Mar. 2, 2016), https://www.wired.com/2016/03/hacker-says-can-hijack-35k-police-drone-mile-away (explaining that the implementation of encryption on pre-existing drones would require either a recall or for operators to download and install firmware updates, which may slow down a drones' responsiveness to commands); Matt Leonard, *Drone Forensics Boosts UAS Defense*, GCN (Sept. 7, 2016), https://gcn.com/Articles/2016/09/07/drone-forensics.aspx (stating that "[a] drone simply lacks the computing ability to handle sophisticated encryption technology"); Alex Perekalin, *Drone Gone in 11 Milliseconds*, Kaspersky Lab (Apr. 19, 2017), https://www.kaspersky.com/blog/drone-gone-in-11-ms/14692 (noting that implementing encryption could require additional energy consumption by the drone and controller).

[30] Gregory S. McNeal, *Key Questions About Securing Drones from Hackers*, Forbes (Oct. 19, 2016), https://www.forbes.com/sites/gregorymcneal/2016/10/19/key-questions-about-securing-drones-from-hackers/#74606b033f3c (attributing these advancements to the rise of Internet of Thing technologies).

[31] *See, e.g.*, April Glaser, *Hackers are Able to Seize Control of Consumer Drones and Make Them Fall from the Sky*, Recode (Oct. 28, 2016), https://www.recode.net/2016/10/28/13406082/hackers-control-consumer-drones-ftc-security (reporting that Parrot AR has implemented encryption to prevent hacking).

Researchers have recommended additional means to prevent drones from being hacked. A "jamming-to-noise (J/N) sensor" within the radio frequency front-end of GPS receivers can detect inauthentic radio signals used for spoofing.[32] Drone manufacturers could also incorporate "multi-system or multi-frequency receiver[s]" that would require a hacker to "simultaneously spoof signals at multiple frequencies and from multiple systems"—a more challenging task than spoofing single-frequency GPS signals.[33] While the full list of means to prevent drones from being hacked is not exhausted here, EPIC highlights that adequate means are available to enable the FAA to promulgate standards to protect public safety and national security from drone hacking.

II. The FAA Must Mandate Security Standards for Surveillance Technology Onboard Drones

Establishing secure connection between drone operators and drones is also imperative to prevent hackers from gaining access to the surveillance technology and data collected and stored onboard drones. Hackers can exploit weaknesses in the surveillance devices mounted to drones to access pictures, recorded or live feed video, or other data.[34] In 2017, researchers from the Federal Trade Commission (FTC) successfully demonstrated how to access and commandeer the video feed of three popular civilian drones by exploiting the drones' unencrypted and non-password protected Wi-Fi access points.[35] Unauthorized access to this equipment could enable widespread privacy invasions and surreptitious monitoring.[36]

[32] *UAS Within the Homeland Hearing*, *supra* note 5, at 20 (statement of Todd E. Humphreys).
[33] *Id.* at 21.
[34] Paganini, *supra* note 19.
[35] Glaser, *supra* note 21.
[36] Michael Kushin, *Drones and Cybersecurity Part 1: The Challenges We Face and Cybersecurity's Role*, Fed. Times (Jan. 6, 2015), http://www.federaltimes.com/story/government/it/blog/2014/12/15/dronesand-cybersecurity-part-1-the-challenges-we-face-and-cybersecuritys-role/20450227.

EPIC continues to recommend that the FAA establish minimum security standards to prevent "unauthorized access to the drone's surveillance capabilities or data collected by the drone."[37] The FAA can establish standards by requiring the encryption of C2 data radio links—a best security practice to protect against remote access attacks.[38] Equally important is requiring that both drones and their remote control software and firmware are up-to-date to mitigate vulnerabilities.[39]

III. The FAA Must Mandate Security Standards for the Collection, Retention, Use, and Disclosure of Data Collected by Drone Surveillance Technology

Both the U.S. government and public have little assurance as to how and where their drone data is being stored, how it is being used, and with whom it is being shared. In 2017, the U.S. Army banned the use of DJI drones and other commercial drones in response to concerns about "how DJI is using the data collected" and whether the Chinese government and Chinese companies had access to the collected data.[40] After Senator Chris Murphy (D-CT) and the U.S. Immigrations and Customs Enforcement raised similar concerns about the threats posed by the data practices of drone manufacturers, the U.S. Department of Defense immediately banned the use of commercial drones.[41] Conversely, "Customers often have little knowledge of where their

[37] EPIC Comments, *supra* note 8, at 16.
[38] AirMap, *Security and the Drone-of-Things* (Apr. 13, 2016), https://www.airmap.com/security-drone-of-things; *see also UAS Within the Homeland Hearing*, *supra* note 5, at 29 (explaining that the surveillance technology onboard drones utilize "existing encryption utilities that are very difficult to crack").
[39] AirMap, *supra* note 38.
[40] Memorandum from the Off. of the Deputy Chief of Staff, Dep't of the Army (Aug. 2, 2017), *available at* https://www.suasnews.com/2017/08/us-army-calls-units-discontinue-use-dji-equipment; *see* Bulletin, SAC Intelligence Prog. L.A., U.S. Immigration & Customs Enf't (Aug. 9, 2017), https://info.publicintelligence.net/ICE-DJI-China.pdf (suggesting that the U.S. Army's memorandum arose from concerns about DJI's use of collected data).
[41] Memorandum from Patrick M. Shanahan, Deputy U.S. Sec'y of Def. (May 23, 2018), *available at* https://www.suasnews.com/2018/06/us-dod-pulls-the-plug-on-cots-drones (suspending the purchase of commercial off-the-shelf drones due to inadequate assessment of their "cybersecurity risks"); *see* Letter from Sen. Chris Murphy to Sec'y of Def. James N. Mattis (May 7, 2018), https://www.murphy.senate.gov/download/drone-letter (expressing concerns about the Chinese government's "massive potential intrusion [on] and exploitation" of information about U.S. critical

data might end up" and remain vulnerable "while D.J.I. and other[] [drone manufacturers] give themselves considerable leeway in . . . their user agreements to transfer data across borders."[42]

Security safeguards should also extend to drone manufacturers' mobile applications, websites, and databases that store information about the drone operator and data collected during drone operation. The FAA should require data security and privacy standards requiring drone manufacturers to implement and effectuate reasonable measures to protect collected data and information about drone operators from unauthorized retention, use, and disclosure. Researchers have discovered multiple ways to hack into drone operators' accounts on DJI's mobile application and website, highlighting new channels for hackers to access personal information about a drone operator, video footage, and flight data.[43] By enhancing security standards for data storage onboard and offboard drones, the FAA can reduce the likelihood that individuals will attempt to hack or crash drones to gain access to collected data.

How information disclosures can enhance public safety and national security

The most dangerous aspect of a drone is the uncertainty as to the identity of the operator and the drone's flight plans, uses, and capabilities.[44] Current regulatory standards inadequately address this danger – there is no requirement for the active remote identification of drones

infrastructure obtained from DJI drones operated by U.S. agencies); Bulletin, *supra* note 40 (concluding with "moderate confidence" that DJI "is providing U.S. critical infrastructure and law enforcement data to the Chinese government" and with "high confidence" that DJI is strategically targeting new customer accounts based on "the account holder's ability to disrupt critical infrastructure").

[42] Paul Mozur, *Drone Maker D.J.I. May Be Sending Data to China, U.S. Officials Say*, N.Y. Times (Nov. 29, 2017), https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html.

[43] Conor Reynolds, *DJI Drone Hack Opens Up Flight and Video Records to Threat Actors*, Computer Bus. Rev. (Nov. 18, 2018), https://www.cbronline.com/news/dji-drone-hack-check-point (explaining how to obtain a cookie identifier from a drone manufacturer's online customer forum to access a drone operator's account and noting that the drone operator "would receive no notification or signs that a threat actor has complete access to their account").

[44] M. Ryan Calo, *The Drone as a Privacy Catalyst*, 64 Stan. L. Rev. Online 29, 32 (2011), http://www.stanfordlawreview.org/wp-content/uploads/sites/3/2011/12/64-SLRO-29_1.pdf ("Virtually any robot can engender a certain amount of discomfort, let alone one associated in the mind of the average American with spy operations or targeted killing.").

operating in the National Airspace. Mandatory drone identification should be established to ensure that authorities are able to counter drone interference with public safety and national security and to reduce the likelihood that individuals resort to dangerous self-help remedies against drones.

Drones are used for innocuous and malicious purposes, but an individual cannot reliably identify these purposes by merely looking at a drone. Innocuous drone uses include crop inspection, rescue operations, and limited forms of real estate photography.[45] Conversely, malicious and intrusive uses of drones are wide-ranging and widespread. Paparazzi, private detectives, commercial entities, stalkers, and criminals can all use drones to collect sensitive personal data.[46] There have already been cases where private individuals discover drones with cameras deployed outside their homes and windows, even those far above ground level.[47] Others have found drones hovering over them outside to capture images of their private activities.[48] There have also been reports from people concerned they are being sexually harassed by drone

[45] Fed. Aviation Admin., *FAA Aerospace Forecast: Fiscal Years 2018-2038*, at 43 (2018), https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2018-38_FAA_Aerospace_Forecast.pdf. *But see* Bulletin, *supra* note 40, at 3 (alleging that Chinese companies began purchasing California vineyards after gaining access to data from a drone used by a Californian wine producer to survey and monitor grape production).

[46] A. Michael Froomkin & P. Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 Conn. L. Rev. 2, 33 (2015), *available at* https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1061&context=fac_articles.

[47] *See, e.g.*, Michael Marois, *Creeps Embrace a New Tool: Peeping Drones*, Bloomberg News (May 5, 2015), https://www.bloomberg.com/news/articles/2015-05-05/creeps-embrace-a-new-tool-peeping-drones; Laura Sydell, *As Drones Fly in Cities and Yards, So Do the Complaints*, NPR (May 12, 2014), http://www.npr.org/sections/alltechconsidered/2014/05/12/311154242/as-drones-fly-in-citiesand-yards-so-do-the-complaints.

[48] *See Hearing on AB 856 Before the Assemb. Comm. on Privacy & Consumer Prot.*, 2 (Cal. 2015), http://www.leginfo.ca.gov/pub/15-16/bill/asm/ab_0851-0900/ab_856_cfa_20150504_121005_asm_comm.html ("Paparazzi . . . have used drones for years to invade the privacy and capture images of public persons in their most private of activities.").

operators.[49] Even Google Executive Chairman Eric Schmidt has recognized that drones can be maliciously used during neighbor disputes to spy on or harass other neighbors.[50]

The inability to identify drone operators and drones' flight plans, uses, and capabilities cause people to perceive drones as threatening and to use dangerous self-help remedies against them.[51] Shooting down drones is the most dangerous self-help remedy used against drones and is becoming increasingly common. In 2015, a Kentucky father was arrested and charged for wanton endangerment and criminal mischief after he shot down a drone flying above his property that he suspected was spying on his 16-year old daughter.[52] Notably, a Kentucky judge dismissed all charges after finding that the drone invaded the father's privacy, thereby justifying the father's use of dangerous self-help remedies.[53] Similarly, in early 2019, a man in Long Island, New York shot down a drone being used to search for a lost dog.[54] The operator of the drone believed that "if [the man] knew the purpose of that drone he wouldn't have shot [it]."[55] In both cases, the shooters could do no more than guess what surveillance devices were enabled on the drones and for what purposes before determining how to act.[56]

[49] *See, e.g.*, Julie Balise, *Woman Claims Drone Harassed Her at Virginia Beach*, Tech. Chron. (May 16, 2014), https://blog.sfgate.com/techchron/2014/05/16/woman-claims-drone-harassed-her-at-virginia-beach.

[50] James Ball, *Google Executive Chairman Say in Guardian Interview that Technology Has Potential to 'Democratise the Ability to Fight War*,' Guardian (Apr. 20, 2013), https://www.theguardian.com/technology/2013/apr/21/drones-google-eric-schmidt.

[51] S*ee* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 1131, 1146 (2011) (indicating that, without certainty as to the capabilities of drones, individuals may suffer "embarrassment, chilling effects, loss of solitude . . . from the mere belief that one is being observed").

[52] Chris Matyszczyk, *Judge Rules Man Had Right to Shoot Down Drone over His House*, CNet (Oct. 28, 2015), https://www.cnet.com/news/judge-rules-man-had-right-to-shoot-down-drone-over-his-house.

[53] *Id.*

[54] *Long Island Man Arrested for Shooting Drone that Looks for Missing Dogs*, CBS: N.Y. (Feb. 24, 2019), https://newyork.cbslocal.com/2019/02/24/arrest-shooting-drone-missing-dog.

[55] *Id.*

[56] EPIC Comments on Clarification of Registration Requirements, *supra* note 7, at 11 ("The public should not be left to wonder what surveillance devices are enabled on the drone flying above their heads."); *see* Froomkin & Colangelo, *supra* note 46, at 22 ("Determining the scope of permissible self-help will always be complicated by the difficulty victims have in trying to ascertain what the invading robot is doing.").

The inability to identify drone operators and to obtain additional information about drones has also interfered with public safety and national security. For example, in 2015, firefighters combatting wildfires were forced to suspend the aerial delivery of 5,000 gallons of fire retardant because a private drone was flying overhead, and "[a]uthorities could not figure out who was flying the drone or where it returned to."[57] In a similar incident, drone operation grounded aerial firefighting operations for fifteen to twenty minutes, burning valuable time "that would have created a much safer environment" and prevented "many citizens [from] running for their lives."[58]

Drones operating in restricted airspace, particularly near airports, also endanger the public and national security. An aerial collision between an airplane and drone, or "drone-strike," can be catastrophic.[59] A study conducted by the FAA and partnering institutions concluded that a drone-strike can cause more severe damage than a bird-strike to an airplane's windshield, wing, and vertical and horizontal stabilizers.[60] Plainly, one pilot has stated, "If a drone hit this airplane in certain spots, I'm not going to be able to control that airplane and I'm going to crash the airplane."[61] In 2017, the FAA received approximately 250 reports of drones operating near

[57] Melissa Pamer & Eric Spillman, *Illegal 4-Foot Drone Shut Down Aerial Firefight over Lake Fire: Forest Service*, KTLA (June 25, 2015), https://ktla.com/2015/06/25/illegal-4-foot-drone-shut-down-aerial-firefight-over-lake-fire-forest-service.

[58] Chris Matyszczyk, *Drones Disrupt Efforts to Fight California Wildfire*, CNET (July 19, 2015), https://www.cnet.com/news/drones-disrupt-efforts-to-fight-california-wildfires.

[59] *See* Sherisse Pham, *Drone Hits Passenger Plane in Canada*, CNN (Oct. 16, 2017), https://money.cnn.com/2017/10/16/technology/drone-passenger-plane-canada/index.html ("If a drone were to hit the window of a cockpit and incapacitate the pilot, or were to damage in anyway an engine, [a drone strike] could have catastrophic results.") (quoting Marc Garneau, Transport Minister, Can.).

[60] Assure, Volume II – UAS Airborne Collision Severity Evaluation – Quadcopter (July 2017), *available at* http://www.assureuas.org/projects/deliverables/a3/Volume%20II%20-%20UAS%20Airborne%20Collision%20Severity%20Evaluation%20-%20Quadcopter.pdf. The study also notes that, unlike bird-strikes, drone-strikes may cause battery fires onboard the struck aircraft. *Id.*

[61] Scott Noll, *Danger in the Skies, Close Calls with Drones Skyrocketing*, ABC: News 5 Cleveland (Feb. 20, 2019), https://www.news5cleveland.com/news/investigations/danger-in-the-skies-close-calls-with-drones-skyrocketing (quoting Denise Hobart, Chief Pilot & President, Am. Winds Aviation).

airports each month.[62] These drone operations have caused significant delays, such as the recent suspension of flights into Newark airport after a drone was reported flying 3,500 feet over another nearby airport.[63]

Current FAA regulations are inadequate to alleviate individual uncertainty regarding drones and to enable the government to effectively address drones flying unlawfully in restricted airspace. As of February 2019, FAA regulations pertaining to drone identification mandate only passive identification, requiring only that a drone be registered and be affixed with registration numbers externally visible.[64] Both EPIC and the FAA's Aviation Rulemaking Committee Working Group 1 have scrutinized passive identification because it is "nearly impossible to read a registration number on a UAS that is more than a few feet away."[65] These passive identification requirements constitute "the bare minimum the government should be doing" because, as it stands, an individual's ability to evaluate the threat posed by a drone and the government's ability to address unlawful and dangerous drone operation are only as great as their

[62] FAA, *UAS Sightings Report*, https://www.faa.gov/uas/resources/public_records/uas_sightings_report (last updated Feb. 15, 2019).
[63] David Shepardson, *FAA Details Impact of Drone Sightings on Newark Airport*, Reuters (Jan. 23, 2019), https://www.reuters.com/article/us-usa-drones/faa-details-impact-of-drone-sightings-on-newark-airport-idUSKCN1PH243; *see also* Feargus O'Sullivan, *Who Keeps Buzzing London's Airports with Drones?*, CityLaw (Jan. 9, 2019), https://www.citylab.com/transportation/2019/01/airport-flight-delay-heathrow-gatwick-security-drones-shutdown/579883 (noting that a drone sighting forced London's Gatwick airport to close for 36 hours, grounding 1,000 planes and affecting approximately 140,000 individuals).
[64] *See* Registration and Marking Requirements for Small Unmanned Aircraft, 80 Fed. Reg. 78,593, 78602–03 (2015), https://www.govinfo.gov/content/pkg/FR-2015-12-16/pdf/2015-31750.pdf; External Marking Requirement for Small Unmanned Aircraft, 84 Fed. Reg. 3669, 3671 (2019), https://www.govinfo.gov/content/pkg/FR-2019-02-13/pdf/2019-00765.pdf (modifying the previous rule that "allowed the registration number to be placed in an enclosed compartment (*e.g.*, the battery compartment on the small unmanned aircraft")).
[65] Aviation Rulemaking Comm., Fed. Aviation Admin., ARC Recommendations Final Report: Appendix B Working Group 1 Report 42 (2017), https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final %20Report%20with%20Appendices.pdf; EPIC Comments on Clarification of Registration Requirements, *supra* note 7, at 12.

eyesight and vision-enhancing tools that enable them to read the registration number on an aloft drone.[66]

EPIC has long advocated that these threats to public safety and national security can be redressed by requiring active remote identification and broadcasting of drone registration information and relevant information to the other drone operators, the public, and the authorities.[67] Drone registration information and relevant information should include the identity of the operator; flight plans and data, such as location of a drone when aloft (latitude, longitude, and altitude), course, and speed over ground; intended use; and capabilities of surveillance technologies. Any drone carrying video surveillance technology would be required to make clear at registration the specific capabilities of the drone, including resolution, frame rate, and zoom range. Any drone carrying audio surveillance technologies would be required to make clear at registration specific capabilities to capture and record audio communications or broadcast. Any drone carrying technology to engage in interception of signal communication, human recognition at a distance, or other advanced surveillance techniques, would be required at the time of registration to detail the capabilities and the anticipated use.

Any change in the functional capability of a drone through the adoption of new capabilities or the deployment of a payload that is different from that stated at the time of the initial registration would require change in the registration information prior to use.

Broadcasting drone registration information enhances public safety and national security by enabling individuals and authorities to identify and evaluate the threat posed by a drone and to

[66] Editorial Board, *The Government's Plan to Register Drones Doesn't Go Far Enough*, Wash. Post (Oct. 26, 2015), https://www.washingtonpost.com/opinions/the-governments-plan-to-register-recreational-drones-doesnt-go-far-enough/2015/10/26/bd21aac8-79c5-11e5-a958-d889faf561dc_story.html?noredirect=on&utm_term=.d38f4beddab4.
[67] EPIC Comments on Clarification of Registration Requirements, *supra* note 7, at 11.

hold drone operators accountable. Remote identification enables individuals to determine whether a drone poses a threat to their safety, privacy, or property, and to seek redress through legitimate legal channels, rather than dangerous self-help remedies.[68] In regard to drones flying in restricted airspace and interfering with public safety and national security, Brian Wynne, president and CEO of the Association for Unmanned Vehicles Systems International, has stated that remote identification could be used to "easily identify a drone's owner and contact them to land the drone if it's flying where it shouldn't."[69]

EPIC commends the FAA's request for information about the development of remote identification technology.[70] The FAA should assess pre-existing remote identification technology, such as the Automated Identification System ("AIS") for commercial vessels,[71] and new technology being developed and tested.[72] DJI is developing a remote identification system that broadcasts a drone's "registration number and other basic information such as its speed, direction, and location" via radio or W-Fi link.[73] Intel has publicly demonstrated its "Open Drone ID" that uses Bluetooth 4.2 broadcast packs and Bluetooth 5 advertising extensions to broadcast a drone's "unique ID, location, direction, altitude, speed, make/model, base location, and other

[68] Richard M. Thompson II, Cong. Research Serv., R43965, Domestic Drones and Privacy: A Primer 6–11 (2015).

[69] Lora Kolodny, *Why Airports Can't Stop Drones from Causing Chaos*, CNBC (Jan. 9, 2019), https://www.cnbc.com/2019/01/08/why-airports-cant-stop-drone-disruptions.html.

[70] FAA, Request for Information on UAS Remote Identification (2018), *available at* https://faaco.faa.gov/index.cfm/announcement/view/32227.

[71] *See* 80 F.R. 5281, amending 33 C.F.R. § 164.46. The ADS-B standard is intended to provide sense and avoid capability for aircraft and may also be deployed for drones. However, it is not designed to provide information about UAS location, course, and speed to the general public. By contrast, information about vessels equipped with AIS is available to the public through freely available apps.

[72] Isabelle Lee, *FAA Issues Request for Information (RFI) from Industry Partners Interested in Developing Remote ID and Unmanned Traffic Management Systems*, UAV Coach (Jan. 24, 2019), https://uavcoach.com/remote-id-faa-rfi.

[73] DJI, *DJI Proposes Systems for Managing and Monitoring Drone Traffic*, DJI: Newsroom News (Sept. 23, 2017), https://www.dji.com/newsroom/news/dji-proposes-systems-for-managing-and-monitoring-drone-traffic.

related data."[74] Moreover, Wing, AirMap, and Kittyhawk have also demonstrated remote identification of drones using a network-based remote ID application utilizing the open-source InterUSS platform.[75] The FAA should encourage the development of remote identification and must establish standards requiring its implementation.

These recommendations fall squarely within the FAA's authority and direction from Congress under the FAA Reauthorization Act of 2018. Section 376 of the Act directs the FAA to develop a plan for the implementation of UAS traffic management (UTM) services that, *inter alia*, permit the testing of remote identification and assess the risks raised and mitigation means required to remotely identify drones.[76] Moreover, the Act directs the FAA to develop plans to implement "data exchange protocols to share UAS operator intent, operational approvals, operational restraints, and other data necessary to ensure safety or security of the National Airspace System."[77] The FAA has the authority and adequate technological means to require active remote identification to enhance public safety and national security.

IV. Conclusion

The FAA should require a secure connection between drones and drone operators and also remote identification and broadcasting of relevant information. Absent such standards, integration of drones into the NAS poses significant safety and privacy risks, undermining public safety and national security. By establishing these security and design standards, the FAA can effectuate its mission to the public.

[74] Mike Rees, *Intel Demonstrates Remote Drone Identification Solution*, Unmanned Sys. Tech. (Aug. 20, 2018), https://www.unmannedsystemstechnology.com/2018/08/intel-announces-new-open-standard-for-remote-drone-identification.
[75] Malek Murison, *AirMap, Kittyhawk, and Wing Demonstrate InterUSS Remote ID Solution*, DroneLife (Jan. 17, 2019), https://dronelife.com/2019/01/17/airmap-kittyhawk-and-wing-demonstrate-interuss-remote-id-solution.
[76] Federal Aviation Administration Reauthorization Act of 2018, Pub. L. No. 115-254, § 376(b)(2).
[77] § 376 (c)(3)(D)(ii).

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow

/s/ Daniel de Zayas
Daniel de Zayas
EPIC Clerk