Brooklyn Law Review

Volume 82 | Issue 3 Article 11

2017

"Big Brother" in the Private Sector: Privacy Threats Under the FAA's New Civilian Drone Regulations

Sean M. Nolan

"Big Brother" in the Private Sector

PRIVACY THREATS UNDER THE FAA'S NEW CIVILIAN DRONE REGULATIONS

INTRODUCTION

With the advent of a mass market for civilian drones in the United States on the horizon, cybersecurity concerns regarding potential data misappropriation are greater than ever before. These concerns were compounded in 2015 when the Federal Aviation Administration (FAA)[1] released a draft of small, unmanned aerial vehicle (drone) regulations for public notice and comment, which, notably, did not include any privacy provisions.[2] Following the FAA's issuance of proposed regulations, the Electronic Privacy Information Center (EPIC), along with a number of other privacy advocacy organizations, commenced a legal action against the FAA, which ultimately sought to force the FAA to include privacy provisions in its new drone regulations.[3] EPIC's petition was dismissed as premature in May of 2016 by the Court of Appeals for the D.C. Circuit, which held that only final regulations may be challenged, and the regulations at issue were still in draft form.[4] Soon after the D.C. Circuit's decision, the FAA announced that it had promulgated a final version of these regulations, which took effect on August 29, 2016.[5] EPIC

---

[1] The Federal Aviation Administration—created by the Federal Aviation Act of 1958—is a federal agency charged with regulating all civil aviation in the United States. *What We Do*, FED. AVIATION ADMIN., https://www.faa.gov/about/mission/activities/ [https://perma.cc/7JL6-HES2].

[2] *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, 183).

[3] *See* Petition for Review, Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., 821 F.3d 39 (D.C. Cir. Mar. 31, 2015) (No. 15-1075), https://epic.org/privacy/litigation/apa/faa/drones/EPIC-v-FAA-DC-Cir-Petition.PDF [https://perma.cc/4UBK-E8YG] [hereinafter First EPIC Petition for Review].

[4] *See* Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., 821 F.3d 39, 43–44 (D.C. Cir. 2016).

[5] Press Release, Fed. Aviation Admin., New FAA Rules for Small Unmanned Aircraft Systems Go Into Effect (Aug. 29, 2016), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20734 [https://perma.cc/LWC7-7WCR].

proceeded to commence a new lawsuit against the FAA, challenging these final drone regulations.[6]

Because the D.C. Circuit dismissed EPIC's concerns as premature during the FAA's drafting stage, which allowed the FAA to promulgate final versions of the regulations as currently drafted, the privacy invasion concerns that were voiced will likely become a reality faster than the rulemakers can respond. With effective legal status, civilian drones will overwhelm our skies, capturing data on a massive scale—data that will subsequently become exposed to hackers.[7] The now-inevitable, wide-scale deployment of civilian drones presents numerous unique and serious problems that the United States is currently ill equipped to handle.

This note provides a criticism of the FAA's new drone regulations with a focus on their disregard for the privacy threats they present. More specifically, it analyzes the privacy concerns presented by civilian drones' vulnerability to hackers. Part I provides background on the growth of the domestic civilian drone industry, the various threats to individual privacy stemming from this growth, and the current state of the law with regard to civilian drone use. Part II analyzes privacy concerns unaddressed by the current legal landscape for civilian drones, with a specific focus on the ability of drones to capture and retain sensitive data that is vulnerable to hackers. Part III discusses the current scope of the FAA's new small civilian drone regulations, and EPIC's legal challenges to the existing regulations as representative of various other civil rights organizations. Finally, Part IV suggests a solution to the major problems posed—identifying potential ways to effectively integrate civilian drones into domestic airspace without eroding the privacy rights of American citizens. First, Congress should amend the existing statute that mandates the FAA to develop drone regulations—or pass a separate statute—to explicitly require that the regulations include privacy protections. Then, after receiving an express grant of congressional authority, the FAA should repeal its current drone regulations, revise them to include privacy provisions, and reopen the revised regulations for public commentary. Statutory action by Congress would force

---

[6] *See* Petition for Review, Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., No. 16-1297 (D.C. Cir. Aug. 22, 2016), https://epic.org/privacy/litigation/apa/faa/drones/EPIC-Petition-08222016.pdf [https://perma.cc/57J6-5GDV] [hereinafter Second EPIC Petition for Review].

[7] *See* Electronic Privacy Information Center, Comments on Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems 1–2, 13–15 (Apr. 24, 2015), http://www.regulations.gov/#!documentDetail;D=FAA-2015-0150-4314 [hereinafter EPIC Comments].

the FAA to issue significant new regulations that adequately quell the large-scale privacy threat presented by civilian drones.

I. CIVILIAN DRONE USE IN THE UNITED STATES AND ITS IMPACT ON PRIVACY RIGHTS

A. The Birth and Development of the Civilian Drone Industry

Largely attributable to globalization and society's headfirst dive into the digital age, technological advancement has occurred at an exponential pace in modern history, with some sources estimating that computer processing ability currently doubles every twelve to eighteen months.[8] The most recent wave of innovation occurred seemingly overnight, with the development of weaponless drones designed for use outside of the military context by both individuals and commercial entities. Merriam-Webster defines "drone," as used here, as "an unmanned aircraft or ship guided by remote control or onboard computers."[9] Unmanned aerial aircrafts have been in use by the military in some capacity for more than one hundred years, with the first recorded military "drone" use dating back to 1849, when the Austrian military deployed approximately two hundred unmanned balloons into Italy.[10] The first true drones were introduced in World War I to carry bombs to a preset destination.[11] Today, the United States military uses remotely controlled drones for a range of purposes, from scouting and reconnaissance to the elimination of enemy targets.[12] Civilian drones are a much more recent innovation; the FAA only approved the use of civilian drones in the United States in 2013.[13]

---

[8] *See* THE EMERGING FUTURE, ESTIMATING THE SPEED OF EXPONENTIAL TECHNOLOGICAL ADVANCEMENT (2012), http://theemergingfuture.com/docs/Speed-Technological-Advancement.pdf [https://perma.cc/PQ8V-CZJ2].

[9] *Drone*, MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/drone [http://perma.cc/U85X-BKZG].

[10] *See* Hugh McDaid et al., *Remote Piloted Aerial Vehicles: An Anthology*, MONASH UNIV., http://www.ctie.monash.edu/hargrave/rpav_home.html#Beginnings [https://perma.cc/L27P-N7VJ].

[11] Jimmy Stamp, *Unmanned Drones Have Been Around Since World War I*, SMITHSONIAN (Feb. 12, 2013), http://www.smithsonianmag.com/arts-culture/unmanned-drones-have-been-around-since-world-war-i-16055939/?no-ist [https://perma.cc/ET9J-JM2T].

[12] *See Unmanned Aerial Vehicles (UAVs), Unmanned Combat Aerial Vehicles (UCAVs) and Drone Aircraft*, MILITARY FACTORY, http://www.militaryfactory.com/aircraft/unmanned-aerial-vehicle-uav.asp [https://perma.cc/5XC5-F4ZR] (listing different types of military drones and their uses).

[13] *See* Joan Lowy, *FAA Certifies First 2 Drones for Domestic Flight*, SAN DIEGO UNION TRIB. (July 26, 2013), http://www.sandiegouniontribune.com/sdut-faa-certifies-first-2-drones-for-domestic-flight-2013jul26-story.html [https://perma.cc/THS2-AGSG].

The transition from expensive, modern military drones, like those deployed by the United States,[14] to affordable drones available for civilian and commercial use has spurred the growth of a new global industry containing heavyweight competitors[15]—one recently valued at approximately $8 billion.[16] As a result, civilian drone development has been occurring at a rapid pace in the United States, and rulemakers have struggled to keep up.[17] Although civil and commercial drone sales currently comprise only about 3.8% of the drone industry,[18] several predictions forecast that this dynamic will shift substantially.[19] While other nations have been utilizing civilian drones for years,[20] and have developed or are developing corresponding regulations to ensure the safe assimilation of drones into their airspaces, the United States' legislative process has been outpaced by technological advancement in this arena.[21] The commercial drone age is only just beginning and the already unprecedented capabilities of these unmanned aerial vehicles will continue to develop as the industry matures.

Civilian drones already on the market have advanced capabilities, including extremely high-definition live feed and recording cameras, infrared ray and heat sensors, and global positioning systems that can track a high volume of targets over a long range.[22] Further, many of these devices are designed

---

[14] For instance, the MQ-9 Reaper—a commonly used United States military drone—reportedly costs $12,548,710.60. *Drones*, TIME (Nov. 6, 2012), http://nation.time.com/2012/11/06/12548710-60/ [https://perma.cc/26W2-BX7L].

[15] *See* Fintan Corrigan, *Big Money Investing in Drones Giving Sector Real Momentum*, DRONEZON (Sept. 3, 2015), http://www.dronezon.com/drone-companies-news-interviews/investing-in-drones-gives-sector-real-momentum/ [https://perma.cc/7MAC-CAGE].

[16] Jack Nicas & Douglas MacMillan, *After Fresh Investment, Chinese Drone Maker DJI Valued at About $8 Billion*, WALL ST. J., http://www.wsj.com/articles/chinese-drone-maker-dji-raises-75-million-from-accel-partners-1430915407 [https://perma.cc/NL9V-GYNU] (last updated May 6, 2015).

[17] *See* BOB HAZEL & GEORGES AOUDE, OLIVER WYMAN, IN COMMERCIAL DRONES, THE RACE IS ON: AVIATION'S FASTEST-GROWING SECTOR OUTPACES US REGULATORS 3 (2015), http://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/apr/Commercial_Drones.pdf [https://perma.cc/JTV6-EEFC].

[18] BILL CANIS, CONG. RESEARCH SERV., R44192, UNMANNED AIRCRAFT SYSTEMS (UAS): COMMERCIAL OUTLOOK FOR A NEW INDUSTRY 6 (2015).

[19] *Id.* at 7 (citing *The Drones Report: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications*, BUS. INSIDER INTELLIGENCE (May 27, 2015), http://www.businessinsider.com/uav-or-commercial-drone-market-forecast-2015-2 [http://perma.cc/WS7Z-F7LR]).

[20] For example, in Japan, drones have been utilized for many years in an agricultural context, and in Canada, they have been used by law enforcement to perform search-and-rescue missions. *See* HAZEL & AOUDE, *supra* note 17, at 3.

[21] *Id.*

[22] *See* EPIC Comments, *supra* note 7, at 5.

to be used as a foundation for additional applications.[23] This allows civilians to use drones in a variety of different contexts, ranging from land surveying[24] to celebrity stalking.[25] The sophisticated tools with which civilian drones are equipped do not provide any significant threat to individual privacy on their own but the privacy threat exists because these capabilities are compounded with their small size, affordability, and exposure to hackers. With available models small enough to fly close to the ground to gather images and information, and affordable enough to be given as holiday gifts, the time may soon come when the most significant invasions of personal privacy are not perpetrated by the NSA, but rather the hobbyist next door. Add drones' vulnerability to hackers into the mix,[26] and the need for clear and uniform drone-specific privacy regulations becomes apparent. In light of civilian drones' dramatic rise, the current regulatory environment civilian drones operate within—at both the state and federal level—inadequately addresses the unique and unprecedented privacy threats presented by the widespread use of these unmanned vehicles.

B. Current State and Federal Regulations

In order to effectively convey the privacy concerns presented by the federal regulatory environment in which drones operate, it is necessary to provide an overview of the interactions between state and federal law in this area. Academics, policymakers, and civil liberties organizations disagree as to whether the authority to regulate drone privacy should fall within federal or state domain.[27] Many proponents for a state-

---

[23] Some of these many applications include: aerial photography and cinematography, wildlife monitoring, mapping, police investigation, and emergency response. *See, e.g.*, AERYON LABS INC., http://aeryon.com/ [https://perma.cc/HVB2-W3TG]; AEROVEL, http://aerovelco.com/Flexrotor.html [https://perma.cc/PM64-2F84]; *Phantom*, DJI, http://www.dji.com/product/phantom/.

[24] *See Surveying & Mapping*, 3D ROBOTICS INC., https://3dr.com/enterprise/industries/survey-mapping/ [https://perma.cc/K27Q-SXT4].

[25] *See* Justin Peters, *Good News for Kanye West: California Bans Paparazzi Use of Drones to Spy on Celeb Homes*, SLATE (Oct. 9, 2015), http://www.slate.com/blogs/future_tense/2015/10/09/california_bans_paparazzi_use_of_drones_to_spy_on_celebrities_at_home.html [https://perma.cc/8LPY-BG2C].

[26] Christian de Looper, *Drones Now Big Hacking Target, First Drone Malware Identified*, TECH TIMES (Feb. 4, 2015), http://www.techtimes.com/articles/30634/20150204/drone-hacking-next-big-security-concern.htm [https://perma.cc/UZ9J-72TP].

[27] *See, e.g.*, Robert A. Heverly, *The State of Drones: State Authority to Regulate Drones*, 8 ALB. GOV'T L. REV. 29, 47 (2015) (arguing that the relatively local nature of drone flight favors state regulation); Margot Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. 57 (2013) (advocating for state regulation of civilian drones); *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*,

centric approach base their arguments on the notion that individual privacy laws have traditionally fallen within the province of the states and that states have a robust common law system governing the invasion of privacy.[28] They further argue that in this early stage of civilian drone privacy regulation, states are in the best position to assume the guinea pig role in experimenting with different types of laws, allowing the federal government to follow a wait-and-see approach.[29] Conversely, leaving drone privacy regulation exclusively within the province of state law has already led to the development of piecemeal laws that vary between states; some argue a federal uniform baseline is necessary to protect the privacy interests of all Americans.[30] Additionally, as many civilian drones will likely operate across state lines, particularly in the commercial context, significant variations in state laws will burden interstate operators. The regulation of civilian drones in United States airspace is clearly in the domain of the FAA—an agency of the federal government—and such power to regulate should necessarily extend to protecting against the privacy threat drones present.

1. Inadequacy of the State Law Landscape

The current state law schemes vary state-by-state and do not contemplate or adequately address many of the new and unique threats posed by drones.[31] Some states provide their residents with general privacy protections under both common law and statutes, typically covering violations such as trespass and certain invasions of an individual's right to privacy.[32] Because civilian drones are such a recent innovation, most state privacy laws specific to trespass by aerial vehicles do not consider the prevalent existence of civilian drones and, instead, focus on traditional, manned aircrafts. Similarly, privacy invasion by civilian drones has received little consideration by

---

ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/drones/ [https://perma.cc/AV8R-WP65] (maintaining the position that the federal government must regulate drone privacy).

[28] *See* WELLS C. BENNETT, BROOKINGS INST., CIVILIAN DRONES, PRIVACY, AND THE FEDERAL-STATE BALANCE 4 (2014), http://www.brookings.edu/~/media/Research/Files/Reports/2014/09/civilian-drones-privacy/civilian_drones_privacy_bennett_NEW.pdf?la=en [https://perma.cc/AW7Y-8QHT].

[29] *Id.* at 6.

[30] *See* Sarah Breitenbach, *States Rush to Regulate Drones Ahead of Federal Guidelines*, PEW CHARITABLE TRUSTS (Sept. 10, 2015), http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2015/09/10/states-rush-to-regulate-drones-ahead-of-federal-guidelines [https://perma.cc/6Y5L-W578].

[31] *See* BENNETT, *supra* note 28, at 4.

[32] *Id.* at 5.

courts.[33] While many states have proposed or enacted legislation concerning civilian drone use in certain niches, such as "requir[ing] law enforcement to get a probable cause warrant before using a drone in an investigation,"[34] comprehensive state laws have been slow to develop.[35]

As of March 2017, thirty-five states had enacted laws regulating civilian drone use within their state borders, but most laws are related to the safety of drone operation, rather than privacy concerns (e.g., a number of state laws make it illegal for drones to interfere with emergency first responders).[36] Further, most of the states that do have drone-specific privacy regulations apply them exclusively to government entities, such as law enforcement.[37] There are exceptions however, as there are some states that do have drone-specific privacy regulations that apply to private actors.[38] Florida is one of these exceptions, having recently enacted a law that prohibits "a person, a state agency, or a political subdivision from using a drone to capture an image of privately owned real property . . . if a reasonable expectation of privacy exists."[39] In California, an existing general privacy statute was amended—expanding the offense from knowing invasions of land to include aerial trespass—in response to widespread paparazzi drone use.[40] While there are certainly arguments to be made for a state-centric approach to drone-specific privacy regulation, the failure of states to take this initiative underscores the need for a uniform federal baseline. To comprehensively highlight the deficiencies in the legal framework that civilian drones operate within, it is necessary to also consider the federal legal landscape.

---

[33] *See* Troy A. Rule, *Airspace in an Age of Drones*, 95 B.U. L. REV. 155, 158 (2015).

[34] Allie Bohm, *Status of 2014 Domestic Drone Legislation in the States*, ACLU (Apr. 22, 2014), https://www.aclu.org/blog/status-2014-domestic-drone-legislation-states [https://perma.cc/PQ8W-CYC3] (footnote omitted).

[35] *See id.*

[36] *Current Unmanned Aircraft State Law Landscape*, NAT'L CONFERENCE OF ST. LEGISLATURES (Mar. 20, 2016), http:// www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx [https://perma.cc/CHL6-6AUC].

[37] For example, Utah restricts where law enforcement—not civilians—may operate drones and collect data. *See* UTAH CODE ANN. §§ 63G-18-101, 63G-18-102, 63G-18-103, 63G-18-104, 63G-18-105 (West 2016); *see also* BENNETT, *supra* note 28, at 2–3 (discussing law enforcement as the target of much state drone privacy legislation).

[38] *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43965, DOMESTIC DRONES AND PRIVACY: A PRIMER 26 (2015).

[39] Surveillance by a Drone Act, S.B. 766, 2015 Leg., Reg. Sess. (Fla. 2015) (codified at FLA. STAT. § 934.50 (2015)).

[40] Assemb. B. 856, 2015–2016 Leg., Reg. Sess. (Cal. 2015).

2. Current Status of Federal Law

At the federal level, the legal status of civilian drones in the United States is somewhat murky but evolving quickly. In response to the emergence of the civilian drone market, Congress passed an enabling statute, known as the FAA Modernization and Reform Act of 2012 (FMRA), directing the FAA to promulgate regulations to allow for the safe and effective integration of civilian drones into American airspace.[41] In relevant part, Section 332 commands the FAA to integrate "civil unmanned aircraft systems in the national airspace," and includes requirements for the FAA's development of comprehensive planning, rulemaking, testing, and reporting to Congress; Section 333 provides the FAA authority to issue exemptions based on specifications it shall determine (e.g., size and weight), and decide whether a certificate of airworthiness is necessary for an exemption to be issued; Section 334 requires administrative guidance and rule development for drones operated by *public agencies*; Section 335 requires the FAA to conduct safety studies on drone operation; and Section 336 prohibits the FAA from regulating model aircrafts that are flown recreationally and satisfy other defined qualifications.[42] The FMRA gave the FAA until September 30, 2015 to "provide for the safe integration of civil unmanned aircraft systems into the national airspace system."[43]

In June 2016—nearly a year after the deadline Congress imposed on the FAA to safely integrate civilian drones into United States airspace—the FAA promulgated a set of final regulations governing nonmilitary drone operation in the United States that did not contain any provisions related to privacy.[44] These final regulations were the subject of substantial contention in their draft phase and remain at the center of an active lawsuit, discussed in Part III.[45] Prior to the FAA's issuance of new regulations, civilian drone use in the United States was illegal as a general matter but allowed in some circumstances under various FAA exemptions.[46] There were multiple ways an operator might receive an exemption: as a recreational operator flying a

---

[41] There are six sections in the FMRA's provisions related to unmanned aircraft systems, Sections 331 to 336, which are located in Subtitle B of Title III. *See* FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11 (amending 49 U.S.C. § 40101).

[42] *Id.*

[43] *Id.* § 332(a)(3), 126 Stat. at 73.

[44] *See* Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. § 107 (2016).

[45] *See infra* Part III.

[46] *See* THOMPSON II, *supra* note 38, at 5.

drone that is designated a "model aircraft" under Section 336 of the FMRA;[47] with a certification of airworthiness under the FAA's limited "experimental" designation;[48] or by falling into an industry the FMRA permits the FAA to exempt for specified purposes.[49] The FAA issued over 5500 exemptions under Section 333 of the FMRA alone[50] to organizations that use drones in industries such as "agricultur[e], real estate, film and broadcasting, oil and gas, and construction activities."[51] Under these legal exemptions, many companies developed and marketed drones for civilian use prior to their general legalization.[52] The current uses and potential future uses for civilian drones in the United States are abundant—ranging from use by the general public looking for a more advanced remote control toy to use by major corporations for agriculture, geographic imaging, and cinematography.[53]

With commercial drone use already widespread across many industries based on the FAA's issuance of exemptions, the industry is poised to grow quickly now that commercial drone use is explicitly legal. Major companies such as Amazon and Google hope to eventually operate commercial drones designed to fly out-of-sight for functions such as package delivery to consumers' homes and street-level geographic imaging.[54] While the FAA currently forbids such "beyond-sight" drone flights, it has opened the door to the possibility of testing this type of usage, likely because of pressure from powerful companies like Amazon and Google.[55]

Former President Barack Obama also demonstrated his concern with the privacy implications of government and civilian drone use, issuing a Presidential Memorandum on that topic directed to all agency heads.[56] Addressing governmental entity drone use, the memorandum required that "agencies shall, prior to deployment of new [unmanned aircraft system (UAS)] technology and at least every 3 years, examine their existing UAS

---

[47] *Id.* at 5–6.

[48] *Id.* at 5 (citing 14 C.F.R. §§ 21.191, 21.193, 91.319 (2012)).

[49] *Id.*

[50] *Authorizations Granted Via Section 333 Exemptions*, FED. AVIATION ADMIN., https://www.faa.gov/uas/beyond_the_basics/section_333/333_authorizations/ [https://perma.cc/95ZY-SXXP].

[51] CANIS, *supra* note 18.

[52] *See id.* at 9–11.

[53] *Id.*

[54] Jack Nicas, *Amazon, Google See Shift in Regulatory Stance on Commercial Drones*, WALL ST. J. (May 5, 2015), http://www.wsj.com/articles/amazon-google-see-shift-in-regulatory-stance-on-commercial-drones-1430864309 [https://perma.cc/T9NK-PH2T].

[55] *Id.*

[56] Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, 2015 DAILY COMP. PRES. DOC. 1 (Feb. 15, 2015).

policies and procedures relating to the collection, use, retention, and dissemination of information obtained by UAS, to ensure that privacy, civil rights, and civil liberties are protected."[57] The memorandum proceeded to impose numerous specific requirements upon these agencies in accordance with that mandate.[58] In its second section, the memorandum addressed privacy concerns associated with civilian drone use, although it provided less specificity in this regard.[59] It stated that "a multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the NAS" must be instituted by the Department of Commerce "[w]ithin 90 days."[60] Acting in accordance with this directive, the National Telecommunications and Information Administration worked with various stakeholders to develop a brief guidance document for civilian drone operators, which it issued in May of 2016.[61]

While this guidance document encourages drone operators to follow "voluntary best practices" to protect the data gathered by their drones, it is far from comprehensive at only eight pages, and does not have the binding effect of law. The potential impact of this document is reduced further under the safe assumption that most civilian drone operators will not seek out or read its text. Although President Obama's memorandum and the corresponding guidance document illustrate the prior administration's concern with the current state of federal drone laws, these documents' ultimate impact will be limited without the support of the current administration. Additionally, because the guidance document does not have the force of law that promulgated regulations do, the enumerated "voluntary best practices" will likely have little impact on the behavior of drone operators. The importance of drone privacy regulation—highlighted by the prior administration's focus on it—supports the need for regulation rather than just guidance.

II. WIDESPREAD DRONE LEGALIZATION WITHOUT ADEQUATE PRIVACY SAFEGUARDS

Upon promulgating the final regulations as drafted, the FAA granted effective legal status to drones, spawning

---

[57] *Id.* at 1–2.
[58] *Id.* at 2–3.
[59] *Id.* at 1–2.
[60] *Id.* at 3.
[61] *See* NAT'L TELECOMM. & INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY (2016).

exponential growth of the civilian drone market. As previously mentioned, the market for civilian drones is forecasted to grow at an annual rate of 19% for the next five years.[62] That expansion, absent any federal privacy regulation, will quickly lead to catastrophic results. Specifically, because today's drones are able to fly so low to capture and retain large amounts of sensitive information with unprecedented technology, and are now becoming common place on such a large scale, they will be vulnerable targets to hackers who can misappropriate that sensitive information.

The advanced and developing technological capacity of civilian drones—discussed in Section II.A below—makes the privacy threat presented by their widespread legalization and deployment a problem of significant proportion that is not adequately addressed by current legislation. The severity of this threat becomes clear when one makes two related considerations: (1) the advanced capabilities civilian drones already have or will have in the future that allow them to gather different types of sensitive information and; (2) the vulnerability of this information to misappropriation by hackers, as discussed in Section II.B.

A. The Technological Capacity of Civilian Drones

Civilian drones already on the market are equipped with top-of-the-line video and audio recording technology.[63] Now that civilian drones have been legalized on a wide scale, more advanced models could come equipped with much greater capabilities in the near future.[64] These technologies will work together to give civilian drones unmatched surveillance ability.[65]

One particularly menacing capability that civilian drones will likely be equipped with in the future is facial recognition software.[66] Today, advanced facial recognition technology is very much a reality and is currently under development for application in a range of different areas. In China, for example, facial recognition technology has been successfully programmed into ATM machines so the unique

---

[62] Nicas, *supra* note 54 (citing *The Drones Report: Market Forecasts, Regulatory Barriers, Top Vendors, and Leading Commercial Applications*, *supra* note 19).

[63] *See, e.g.*, Seamus Payne, *7 High Tech Drones for Sale Today*, THE COOLIST (May 1, 2013), http://www.thecoolist.com/7-high-tech-drones-for-sale-today/ [https://perma.cc/44UY-HUVK].

[64] For example, there are already civilian drones that are equipped with advanced video cameras capable of facial recognition being marketed to hobbyists. *See, e.g.*, HOVER CAMERA, https://gethover.com/shop/product/hover-camera [https://perma.cc/LS34-6DNK].

[65] *See* EPIC Comments, *supra* note 7, at 5.

[66] *Id.*

facial features of individuals withdrawing money can be matched with photos contained in the computer's database.[67] Certain international airports in the United States have also recently begun employing facial recognition technology to identify counterfeit passports.[68] Without diving deeply into the functions that enable machines to recognize faces, the technology can be divided into two categories—facial recognition based on features (geometric) and facial recognition based on appearance (photometric).[69] In 2001, facial recognition technology was advanced significantly by computer scientists who developed an algorithm that could identify different faces based on variations of light on different parts of the human face.[70] In 2015, a new algorithm was developed that had the ability to quickly and accurately detect individual faces in a large crowd from many angles.[71] And now, software with that programming has been added to the arsenal of technology being built into civilian drones.[72]

The U.S. military has already developed and programmed highly advanced autonomous drones with facial recognition software that can be used to identify and track targets over long ranges.[73] If domestic law enforcement agencies begin implementing similarly advanced facial recognition technology, it is not difficult to imagine the realistic possibility that any individual's activity could be subject to drone surveillance, absent comprehensive federal laws restricting such drone use. Outside the government context, drones with facial recognition technology may be utilized for the purpose of gathering unique information on large numbers of people without their consent, which could then be used in

---

[67] *See* Hannah Osborne, *China Unveils World's First Facial Recognition ATM Machine*, INT'L BUS. TIMES (May 31, 2015), http://www.ibtimes.co.uk/china-unveils-worlds-first-facial-recognition-atm-machine-1503706 [http://perma.cc/3SVC-GV5K].

[68] *See* Andrea Noble, *U.S. Airports to Roll Out Facial-Recognition Software to Catch Fake Passports*, WASH. TIMES (Jan. 21, 2016), http://www.washingtontimes.com/news/2016/jan/21/us-airports-roll-out-facial-recognition-software/ [https://perma.cc/6EBT-XMNA].

[69] *See* FBI, FACE RECOGNITION, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/face-recognition.pdf [https://perma.cc/Y2CE-VS7G].

[70] *See* Lisa Vaas, *Breakthrough in Facial Recognition: The 'Deep Dense Face Detector'*, NAKED SEC. (Feb. 19, 2015), https://nakedsecurity.sophos.com/2015/02/19/breakthrough-in-facial-recognition-the-deep-dense-face-detector/ [https://perma.cc/FN6B-P7HG].

[71] *Id.*

[72] *See* Justin Lee, *Public Drones Equipped with Facial Recognition Software Raise Privacy Concerns*, BIOMETRIC UPDATE.COM (May 7, 2015), http://www.biometricupdate.com/201505/public-drones-equipped-with-facial-recognition-software-raise-privacy-concerns [https://perma.cc/6WLS-CJ78].

[73] *See* Matthew Rosenberg & John Markoff, *The Pentagon's 'Terminator Conundrum': Robots That Could Kill on Their Own*, N.Y. TIMES (Oct. 25, 2016), https://www.nytimes.com/2016/10/26/us/pentagon-artificial-intelligence-terminator.html [http://perma.cc/Z4WF-CCVT].

combination with existing data for a variety of purposes, such as advertisement targeting. This may seem benign enough, particularly considering that there are already technologies employed by marketers to gather identifying user information on the Internet.[74] Yet, a fleet of drones armed with advanced facial recognition technology and other complementary capabilities could be used to provide information about civilians at a much greater level of detail—a level that would make most people uncomfortable. While the prospect of providing legitimate entities new windows into our personal lives is itself disconcerting, the more significant threat stems from illegitimate uses of this technology—e.g., perpetrating crimes like identity theft.

Many civilian drones currently on the market now come factory-equipped with 4K cameras, which record images and video in ultra high definition.[75] The ability to capture such high-resolution footage allows drones to conduct surveillance from great heights[76] without being noticed by potential targets. And while this functionality could prove beneficial for use in law enforcement[77] and other areas, it could also be used to spy on individuals without their knowledge. Considered in light of widespread drone legalization, the prospect of many civilian drones possessing exceptional surveillance ability becomes daunting.[78] The vulnerability of advanced civilian drones to misappropriation by hackers exponentially increases the privacy threat such drones present.

B. Vulnerability to Hackers

In its comment on the FAA's draft drone regulations,[79] and again in its recent argument to the D.C. Circuit, EPIC mentioned the risk posed by hackers who can obtain sensitive

---

[74] *See* E.J. Schultz, *Facial-Recognition Lets Marketers Gauge Consumers' Real Responses to Ads*, ADVERTISING AGE (May 18, 2015), http://adage.com/article/digital/facial-recognition-lets-marketers-gauge-real-responses/298635/ [https://perma.cc/Q8EV-B94B].

[75] *See* Fintan Corrigan, *4K UHD Video Drones Creating Waves in Aerial Cinematography*, DRONEZON (Oct. 18, 2016), http://www.dronezon.com/aerial-photo-and-video/aerial-filming/4k-ultra-high-definition-video-drones-creating-waves-in-aerial-cinematography/ [https://perma.cc/4XNK-4GS9].

[76] *See* Stephan Jukic, *The Powerful Potential of 4K Cameras in Crime Detection*, 4K (Dec. 1, 2014), http://4k.com/news/the-powerful-potential-of-4k-cameras-in-crime-detection-4335/ [https://perma.cc/ZMW5-E5DC].

[77] *See id.*

[78] It is not difficult to imagine some of the illegitimate uses of drone surveillance technology, ranging from recording conversations intended to be private, to targeting and stalking individuals for violent purposes.

[79] *See* EPIC Comments, *supra* note 7, at 13–15.

information from drones.[80] Citing a report that analyzed the drone hacking research of Todd Humphreys,[81] EPIC argued that this risk is due, in large part, to the relative ease with which drones can be hacked.[82] Humphreys has received substantial recognition for his expertise in GPS technology, and has even delivered a TED Talk[83] on how a GPS can be manipulated.[84] The Department of Homeland Security took interest in his research, which demonstrated the ease with which a drone's GPS can be hacked. At the Department's request, Humphreys provided a live demonstration, where he hacked into a drone's GPS and commandeered it.[85] Humphreys's demonstrated expertise in manipulating drone technology captured the attention of Congress. In March of 2015, Humphreys was called to testify about the threat of drone hacking before the House Subcommittee on Oversight and Management Efficiency of the Committee on Homeland Security.[86]

The report cited by EPIC stated that "Humphrey[s] demonstrated to Homeland Security agents that [by] spending around $1,000 on equipment and designing an application able to send signals to the drone's GPS receiver he is able to gain complete control of the vehicle."[87] Humphreys continued: "[I]f you can commander the GPS unit, then you can basically spoon feed false navigation information in the navigation center of

---

[80] *See* Brief for Petitioner at 9–10, Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., 821 F.3d 39 (D.C. Cir. Sept. 28, 2015) (No. 15-1075), https://epic.org/privacy/litigation/apa/faa/drones/1575326-EPIC-Opening-Brief.pdf [https://perma.cc/5CXT-B9TZ] [hereinafter EPIC Opening Brief].

[81] Humphreys is an Associate Professor of Engineering at the University of Texas at Austin where he also directs the Radionavigation Laboratory. *See Todd E. Humphreys*, UNIV. OF TEX. AT AUSTIN, https://www.ae.utexas.edu/faculty/faculty-directory/humphreys [https://perma.cc/QPX3-2EVD]. His research focuses on robotics, controls, and orbital mechanics. *Id.*

[82] *See* EPIC Opening Brief, *supra* note 80, at 9–10 (citing Pierluigi Paganini, *Hacking Drones . . . Overview of the Main Threats*, INFOSEC INST. (June 4, 2013), http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/ [https://perma.cc/TYL7-CKFP]).

[83] TED—an acronym for Technology, Entertainment, and Design—"is a [global] nonprofit devoted to spreading ideas, usually in the form of short, powerful talks." *Our Organization*, TED, http://www.ted.com/about/our-organization [https://perma.cc/3B33-4C2R].

[84] *Todd Humphreys*, TED, https://www.ted.com/speakers/todd_humphreys [https://perma.cc/6CD5-ZDAN].

[85] *See Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV*, UNIV. OF TEX. AT AUSTIN AEROSPACE ENG'G & ENG'G MECHANICS (June 28, 2012), http://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing [https://perma.cc/HS22-EMZ4].

[86] *See Todd Humphreys to Testify Before U.S. Congress on UAV Threats*, UNIV. OF TEX. AT AUSTIN AEROSPACE ENG'G & ENG'G MECHANICS (Mar. 17, 2015), https://www.ae.utexas.edu/news/820-humphreys-congress-testimony-2015 [https://perma.cc/H4MK-BLDX].

[87] Paganini, *supra* note 82.

these drones."[88] Hijacking drones in this way is known as "GPS spoofing" and involves intercepting the GPS signals they emit.[89] Various studies have been conducted on the GPS spoofing of drones,[90] and four professors of computer science have published a step-by-step manual detailing how to conduct this type of attack on both civilian and military drones.[91] One prominent member of the international robotics community even stated that "[i]t's easy to spoof an unencrypted drone."[92] Although "easy" is relative, an ordinary civilian likely does not possess the technical expertise to successfully hack a drone, though a few individuals with malicious intent could present an extraordinary threat. Even heavily encrypted United States government data is not hack-proof.[93] Thus, it does not take an abundance of creativity to imagine the risks posed by data-carrying civilian drones, including the potential capture and distribution of unauthorized surveillance video and identity misappropriation.

As EPIC highlighted in its brief, "[w]hen a drone is hacked, it can provide access to pictures, recorded or live feed video, or other sensitive personal information."[94] Taking this a step further, it is not a stretch to envision governmental actors from adversarial nations or extremists unconcerned with American laws using this relatively simple hacking method to access civilian drones. And while the prospect of U.S. enemies commandeering civilian drones flying over domestic skies presents obvious direct safety threats, if those individuals were to acquire massive quantities of data from civilian drones in large scale and coordinate information attacks, the security of the United States as a nation could be put in jeopardy. The vulnerability of drones to hacking has even been evidenced on multiple occasions in a military context. In 2009, Iraqi insurgents, using readily available software, successfully gained

---

[88] *Id.* (quoting Humphreys).

[89] *See id.* at 9.

[90] *See, e.g.*, Andrew J. Kerns et al., *Unmanned Aircraft Capture and Control Via GPS Spoofing*, 31 J. FIELD ROBOTICS 617 (2014); Daniel P. Shepard et al., *Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks*, 5 INT'L J. CRITICAL INFRASTRUCTURE PROTECTION 146 (2012).

[91] *See* Nils Ole Tippenhauer et al., *On the Requirements for Successful GPS Spoofing Attacks*, CCS '11 PROC. 18TH ACM CONF. ON COMPUTER & COMM. SECURITY, Oct. 17–21, 2011, at 75.

[92] Paganini, *supra* note 82 (quoting Noel Sharkey, cofounder of the International Committee for Robot Arms Control).

[93] *See* Julie Hirschfeld Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (July 9, 2015), http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?_r=0 [http://perma.cc/A34L-UWH5].

[94] *See* EPIC Opening Brief, *supra* note 80, at 10.

access to unencrypted live video from U.S. Predator drones.[95] In 2011, Iran captured a U.S. spy drone, which it alleged was a result of spoofing the drone's heavily encrypted GPS (although the United States has maintained that the drone's crash landing and capture was caused by a mechanical error).[96] Then, in 2013, Iran released footage it alleged to have recovered from the drone.[97] Considering that hackers have gained access to expensive and heavily protected military drones on several reported occasions, individuals hostile to the United States can likely access the much less protected civilian drones flying in U.S. airspace.[98]

Because many lawful civilian drones will capture and retain private and potentially dangerous information, their exposure to individuals skillful enough to gain access to their operating systems presents major risks to U.S. safety and privacy.

III. PRIVACY IGNORED: EPIC'S MULTIYEAR LEGAL BATTLE AGAINST THE FAA AND THE FAA'S AGGRAVATION OF EPIC'S PRIVACY CONCERNS

A. EPIC's 2012 Petition, the FAA's Subsequent Civilian Drone Regulations, and the Resulting Lawsuits

Following Congress's passage of the FMRA in 2012, privacy and civil liberties organizations vocalized their concerns with the act. Soon after the FMRA was enacted, EPIC and numerous other organizations dedicated to civil liberties, human rights, technology, and consumer rights sent a petition to the FAA requesting that the FAA "address the threat to privacy and civil liberties that will result from the deployment of aerial drones within the United States."[99] In this petition, EPIC and other represented organizations identified specific threats to privacy stemming from the widespread commercialization of

---

[95] *See* Siobhan Gorman et al., *Insurgents Hack U.S. Drones—$26 Software Is Used to Breach Key Weapons in Iraq; Iranian Backing Suspected*, WALL ST. J. (Dec. 17, 2009), http://www.wsj.com/articles/SB126102247889095011 [https://perma.cc/8ZPM-LG9M].

[96] *See* Gordon Corera, *Iran Shows 'Hacked US Spy Drone' Video Footage*, BBC (Feb. 7, 2013), http://www.bbc.com/news/world-middle-east-21373353 [https://perma.cc/6M95-9SY5].

[97] *Id.*

[98] For example, Mexican drug cartels have been reportedly crossing the United States-Mexico border with ease by hacking into and diverting nonmilitary drones utilized by the United States Border Patrol. *See* Waqas Amir, *US Border Patrol Drones Hacked by Drug Cartels*, HACKREAD (Jan. 3, 2016), https://www.hackread.com/us-border-patrol-drones-hacked-by-drug-cartels/ [https://perma.cc/U8UD-UQNF].

[99] *See* Petition from EPIC, et al. to the United States Federal Aviation Administration, at 1 (Feb. 24, 2012) [hereinafter EPIC Petition to the FAA].

drones, highlighting that these drones are "designed to undertake constant, persistent surveillance to a degree that former methods of aerial surveillance were unable to achieve."[100]

The petition starts by acknowledging that civilian drone use is growing in the United States, and then transitions to briefly discussing the "[s]ubstantial [t]hreats to [p]rivacy" posed by drones in light of the industry's growth.[101] The petition identifies the unparalleled domestic surveillance capabilities possessed by drones as its foremost threat, which can "provide real-time video streams at a rate of 10 frames a second."[102] It raises further concerns with drones' ability to track multiple targets over a long range using advanced technology such as "infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers."[103] These capabilities allow drones to obtain a wide range of data,[104] which would become vulnerable should a drone equipped with some or all of these capabilities fall into the hands of a hacker.[105] The petition also conveys that the privacy threat presented by the unique capabilities of drones is heightened by their ability to "operate undetected in urban and rural environments."[106]

Based on these concerns, EPIC requested the agency take action in the form of "a notice and comment rulemaking" period in relation to the privacy implications of private and government use of civilian drones in the United States.[107] It then suggested that the primary privacy considerations of that rulemaking period should be "the use and retention of data acquired by drone operators; the relation between drone

---

[100] *Id.* at 3.

[101] *Id.* at 2.

[102] *Id.* (quoting *U.S. Army Unveils 1.8 Gigapixel Camera Helicopter Drone*, BBC NEWS (Mar. 8, 2012), http://www.bbc.co.uk/news/technology-16358851 [https://perma.cc/UV83-Q6WN]).

[103] EPIC Petition to the FAA, *supra* note 99, at 2–3.

[104] Equipped with the proper technology, drones can be used to obtain massive amounts of data for a variety of purposes, ranging from topographic mapping to accident investigation for insurance providers. For a discussion of some of the various applications of data-capturing drones, see Stuart Thornton, *Data Drones*, NAT'L GEOGRAPHIC (May 5, 2014), http://nationalgeographic.org/news/data-drones/ [https://perma.cc/9DQW-X7EN].

[105] Many technology experts familiar with drone technology voice similar concern over drones' exposure to being hacked. *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/ [https://perma.cc/KW22-XFFH]; Mary Shacklett, *Drones Collecting Big Data Present New Security and IT Concerns*, TECHREPUBLIC (Feb. 16, 2016), http://www.techrepublic.com/article/drones-collecting-big-data-present-new-security-and-it-concerns/ [http://perma.cc/TZ9X-95Q4].

[106] EPIC Petition to the FAA, *supra* note 99, at 3 (quoting Jennifer Lynch, *Are Drones Watching You?*, ELEC. FRONTIER FOUND. (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you [https://perma.cc/2SFH-4Q8X]).

[107] *Id.* at 5.

operation and property rights; the ability of an individual to obtain a restraining order against a drone vehicle; and use limitations on drone vehicles and requirements for enforcement of those limitations."[108] If the FAA were to consider these aspects, it would necessarily focus much more acutely on the potential privacy implications of civilian drone legalization.

The FAA denied this petition and stated that privacy issues raised by EPIC and the petition's other signatories are "not an immediate safety concern."[109] The FAA then proceeded to draft the FMRA-mandated regulations without incorporating provisions related to EPIC's privacy concerns[110] and posted them for public comment in February of 2015.[111] The comment period closed two months later.[112] The drafted rules focused entirely on conventional safety issues presented by the legalization of drones for private use, setting weight, height, and speed limits for these unmanned aerial vehicles.[113] These rules also proposed a licensing program for drone operators, subject to oversight by the Transportation Authority Administration, and enumerated other restrictions on drone operation, including a ban on flying drones outside the operator's line of sight.[114] In overwhelming response to the FAA's posting of these proposed rules, more than 4500 comments were received.[115] EPIC was among these commentators, posting a seventeen-page comment with arguments

---

[108] *Id.*

[109] Letter from Lirio Liu, Dir. of Office of Rulemaking for the Fed. Aviation Admin., to Marc Rotenburg, EPIC Exec. Dir., & Amie Stepanovich, EPIC Nat'l Sec. Counsel (Nov. 26, 2014), https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf [https://perma.cc/2E3R-PPQY].

[110] *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544, 9544–51 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107 & 183).

[111] *Operation and Certification of Small Unmanned Aircraft Systems*, REGULATIONS.GOV, http://www.regulations.gov/#!documentDetail;D=FAA-2015-0150-0017 (last visited June 13, 2017).

[112] *Id.*

[113] *See* Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. at 9546, 9551–52.

[114] *Id.* at 9546–47.

[115] Of the six major rules the Department of Transportation (DOT) and its agencies have issued since the start of 2015, the FAA's rule governing the operation of small unmanned aircraft systems received the most commentary in its proposal stage—more than twice as many comments as the second most commented-on major rule issued by the DOT in that span. For a list of the DOT's major rules, see U.S. GOV'T ACCOUNTABILITY OFF., http://www.gao.gov/legal/congressional-review-act/ (select "Department of Transportation" in the "Agency" dropdown; then select the "Major" button next to the "Rule Type" category; then input the relevant date range for the "Date Published in the Federal Register" category, inputting a start date of 01/01/2015; then click "Search"). For a quantification of the comments on each major FAA regulation since the start of 2015, see *Operation and Certification of Small Unmanned Aircraft Systems*, *supra* note 111.

in support of their position that the FAA should amend these rules to include comprehensive privacy provisions.[116]

In March of 2015, prior to the FAA's closure of the notice and comment period for these draft regulations, EPIC, along with various other privacy organizations, initiated a civil action against the FAA in the United States Court of Appeals for the D.C. Circuit.[117] This petition essentially argued that the FAA was legally mandated to regulate privacy in its drone rules and, consequently, EPIC requested that the court require the FAA to revise its proposed regulations.[118] Within two months, the FAA moved to dismiss this suit.[119] In the motion, the FAA took the position that EPIC's lawsuit was premature, as no final rule had yet been issued.[120] The FAA also refuted EPIC's claim that its request to initiate a new rulemaking was improperly denied, arguing that EPIC's request was brought too late, as it was not filed within the required sixty-day time frame.[121] After a round of briefing and argument by both parties,[122] the D.C. Circuit granted the FAA's motion to dismiss in May of 2016.[123] The D.C. Circuit left the door open for EPIC to renew its challenge after the FAA's issuance of final rules, resting its decision on well-established law that only final agency rules are reviewable by a court.[124]

Following the D.C. Circuit's decision, the FAA acted promptly in promulgating the final regulations without any privacy provisions, which became effective on August 29, 2016.[125] Without wasting any time, EPIC renewed its challenge in the D.C. Circuit—now attacking the final regulations.[126]

---

116 EPIC Comments, *supra* note 7, at 1.

117 *See* Daniel Wilson, *Aerospace and Defense Cases to Watch in 2015's 2nd Half*, LAW360 (Aug. 24, 2015), http://www.law360.com/articles/687030/aerospace-and-defense-cases-to-watch-in-2015-s-2nd-half [https://perma.cc/8DUB-VXME].

118 *See* First EPIC Petition for Review, *supra* note 3, at 2.

119 Motion to Dismiss, Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., 821 F.3d 39 (D.C. Cir. May 15, 2015) (No. 15-1075), https://epic.org/privacy/litigation/apa/faa/drones/1552818-Motion-to-Dismiss.pdf [https://perma.cc/YR7C-7KS5].

120 *See id.* at 2.

121 *Id.*

122 EPIC filed its opening brief on September 28, 2015. *See* EPIC Opening Brief, *supra* note 80. On November 4, 2015, the FAA filed its opposition papers. *See* Brief for Respondents, Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., 821 F.3d 39 (D.C. Cir. Nov. 4, 2015) (No. 15-1075), https://epic.org/privacy/drones/epicvfaa/1581988-FAA-Brief.pdf [https://perma.cc/XP6D-L5V2] [hereinafter FAA Opposing Brief].

123 *See* Elec. Privacy Info. Ctr. v. Fed. Aviation Admin., 821 F.3d 39 (D.C. Cir. 2016).

124 *Id.* at 44.

125 *See* Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. § 107 (2016).

126 *See* Second EPIC Petition for Review, *supra* note 6, at 1.

B. Weighing the Parties' Respective Legal Positions

In considering the likely outcome of this now pending action, a brief assessment of the legal positions of the opposing parties is helpful. Academics have made persuasive arguments that the enabling statute, as written, does not provide the FAA authority to regulate drone privacy.[127] By its plain language, the FMRA covers only drone safety, and does not mandate that the FAA take drone privacy issues into account in their regulations. Like many federal statutes, it is broad and categorical, giving the FAA significant flexibility in determining exactly what provisions are necessary to safely integrate civilian drones into national airspace. In summary, the FMRA directs the FAA to "'define the acceptable standards of operation and certification' of drones and to 'establish standards and requirements for operator[s] and pilot[s]' of drones, as well as identify 'the best methods to ensure safe operation' of drones in the [National Airspace System]."[128] The FAA has interpreted this mandate as applying only to conventional airspace safety, meant to prevent casualties that could result from collisions with manned aircraft vehicles or inanimate objects.[129] In contrast, EPIC has maintained the position that "safety" should be more broadly interpreted to include the protection of individual privacy rights.[130] It is not implausible that Congress's failure to include explicit privacy language was intentional—perhaps there was concern about infringing on First Amendment protections, or there simply was not enough bipartisan support.

While the basis of EPIC's position—that a lack of privacy provisions in the FAA's drone regulations could present major problems—is difficult to dispute, its arguments based on the statutory construction of the FMRA and legislative intent may not prevail. In its initial brief, EPIC took the position that the FAA's failure to include privacy considerations in its rulemaking was an error of law and in violation of its congressional mandate.[131] In response to EPIC's brief in the prior action, the FAA argued that EPIC's substantive claims had no

---

[127] *See* Marc Jonathan Blitz et al., *Regulating Drones Under the First and Fourth Amendments*, 57 WM. & MARY L. REV. 49, 50 (2015) ("The Agency, however, would likely need further congressional action before it can restrict UAV flight based on privacy rather than safety concerns.").

[128] EPIC Comments, *supra* note 7, at 2–3 (first and second alterations in original) (quoting FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(a)(1)(A), 126 Stat. 11, 73).

[129] *See* FAA Opposing Brief, *supra* note 122, at 14–18.

[130] *See* EPIC Comments, *supra* note 7, at 7–8, 10–15.

[131] *See* EPIC Opening Brief, *supra* note 80, at 24.

merit as the FAA acted well within its authority in determining that it was not provided any congressional directive to include privacy protections in its regulations.[132]

In interpreting the FMRA, EPIC focused on the word "comprehensive" in the section stating that "[t]he FAA 'shall develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system.'"[133] EPIC argued that Congress consciously decided to use the word "comprehensive" and, in doing so, intended the broad language to encapsulate both safety and privacy considerations.[134] Although EPIC's statutory interpretation is logical, it faces an uphill battle in making this argument in light of the broad deference granted to agency rulemaking under the *Chevron* doctrine.[135] Under *Chevron*, courts first consider Congress's expressed intent in interpreting a statute, and must adhere to that intent.[136] If Congress is silent as to a particular ambiguous issue, courts will grant an administrative agency wide interpretive latitude if the agency's interpretations are "based on a permissible construction of the statute," a relatively low bar.[137] Further, as the FAA pointed out, in *Massachusetts v. EPA*, the Supreme Court instructed courts to apply greater deference to an agency's inaction—like the FAA's refusal to promulgate privacy-specific drone regulations—than they would to an agency's affirmative actions.[138] Thus, EPIC may have difficulty overcoming the deferential standard applied to administrative agencies like the FAA in interpreting statutes they are charged with administering. And if the D.C. Circuit does not side with EPIC in its renewed civil action against the FAA, prompt congressional action will be required to force the FAA to promulgate new drone privacy regulations.

C. Augmented Threat Under the Proposed Regulatory Framework

In the event of the FAA's success on the merits in the renewed *EPIC v. FAA* action, the final regulatory framework it has issued for civilian drones—which sidesteps the privacy concerns outlined in the previous section—will remain in effect.

---

[132] *Id.* at 5–6.

[133] *Id.* at 34 (emphasis omitted) (quoting FAA Modernization Act § 332(a)(i)).

[134] *See id.* at 35.

[135] *See* Chevron USA v. Nat. Res. Def. Council, Inc., 467 U.S. 837 (1984).

[136] *Id.* at 842–43.

[137] *Id.*

[138] *See* FAA Opposing Brief, *supra* note 122, at 11 (citing Massachusetts v. EPA, 549 U.S. 497, 527–28 (2007)).

The FAA justified the absence of privacy provisions from its regulations by maintaining that drone privacy issues are beyond the scope of the rulemaking authority it has been conferred by Congress, and that it has acted within the bounds of its delegated discretion in denying EPIC's 2012 petition.[139] In that denial, the FAA emphasized that, in considering the relative insignificance of the privacy issues raised by EPIC, and its limited available resources, regulating drone privacy concerns is not a priority.[140]

The new regulatory framework provides current market leaders the legal stability necessary to vastly increase their civilian drone production and has opened the gates for many new companies to enter the market. Heightened competition will continue to increase the speed of innovation in the industry and new technology will be implemented faster than lawmakers can respond. If EPIC's renewed suit is decided in favor of the FAA, and the FAA is not otherwise required to regulate drone privacy, any remaining uncertainty in the market will be eliminated, and its growth will occur unfettered. Although a robust civilian drone market may prove beneficial to the U.S. economy, privacy violations and data misappropriation may begin to occur on an unparalleled scale as this market grows without federal drone privacy regulation. Unless Congress and the FAA change course and take substantial preventative measures, the United States will be unprepared to effectively counteract and address major data breaches that occur.[141]

IV. A MULTITIERED SOLUTION

A top-down legislative approach requires Congress to be vigilant in either amending the FMRA, as it currently exists, or enacting new legislation requiring the FAA to include privacy provisions in its regulations. Prior to that action being taken, Congress should exercise its legislative authority to force the FAA to repeal its existing small civilian drone regulations, thereby reinstituting a temporary ban on non-exempted civilian drones. Once a congressional mandate to regulate drone privacy is in place, the FAA will face pressure to revise its drone rules quickly

---

139 *See id.* at 5–6.

140 *See* Letter from Lirio Liu, Dir. of Office of Rulemaking for the Fed. Aviation Admin., to Marc Rotenburg, EPIC Exec. Dir., & Amie Stepanovich, EPIC Nat'l Sec. Counsel, *supra* note 109 ("After reviewing your request, we have determined that the issue you have raised is not an immediate safety concern.").

141 Such data breaches are not speculative. For example, drug cartels have hacked United States Border Control drone data so traffickers are able to discretely cross the United States-Mexico border. *See* Shacklett, *supra* note 105.

to allow the civilian drone market to resume its growth. This section suggests the particular content of these privacy provisions.

A. Congressional Enabling Statute

Although Congress did not expressly mandate that the FAA include privacy provisions in its FMRA regulations, it does not change the importance of privacy protections prior to widespread drone legalization. Accordingly, the first step in averting a potential crisis requires a command from Congress, in the form of either an amendment to the FMRA or a new statute, that the FAA include comprehensive privacy protections in its regulations.

Congressional action that has already been taken indicates that the privacy threat presented by the widespread legalization of civilian drones is on the mind of at least some legislators.[142] Senator Ed Markey and Representative Peter Welch have sponsored numerous subsequent bills to address drone privacy concerns, albeit to little avail.[143] Notably, the Drone Aircraft Privacy and Transparency Act of 2015 sought to amend the FMRA to direct the Secretary of Transportation to study and identify "any potential threats to privacy protections posed by the integration of unmanned aircraft [drone] systems into the national airspace system."[144] It would have also mandated "procedures to ensure that the integration of unmanned aircraft systems into the national airspace system is done in compliance with privacy principles."[145] These bills have yet to become law, but their sponsors are not giving up in their pursuit of amending the FMRA. In March of 2017, Senator Markey and Representative Welch reintroduced their bicameral legislation.[146]

To effectively initiate reparation, Congress will need to engage in a bipartisan effort and seriously consider the drone privacy bill already before them. The Drone Aircraft Privacy Act of 2017 is explicit in its instructions and comprehensive in its scope. It seeks to add numerous sections to the FMRA including one that would require the Secretary of Transportation to establish rules that account for privacy concerns.[147] The bill also

---

[142] *See, e.g.*, Drone Aircraft Privacy and Transparency Act of 2015, S. 635, 114th Cong. (2015); Drone Aircraft Privacy and Transparency Act of 2015, H.R. 1229, 114th Cong. (2015).

[143] Drone Aircraft Privacy and Transparency Act of 2015, S. 635.

[144] *Id.* § 3.

[145] *Id.*

[146] Drone Aircraft Privacy and Transparency Act of 2015, S. 631, 115th Cong. (2017).

[147] *Id.* § 3.

provides some guidance on privacy considerations that should be made in the new rules, specifically regarding data collection restrictions, drone operator disclosure requirements, and surveillance limitations.[148] As of mid-March 2017, the bill was being considered by a designated congressional committee.[149] Whether through this bill or one like it, congressional action is the necessary first step toward protecting the privacy interests of Americans from the new threat presented by civilian drones.

B. Revised Rulemaking by the FAA

Once given clear regulatory authority, the FAA should issue privacy rules governing small civilian drones. The privacy provisions in the new regulatory scheme should include comprehensive standards that focus separately on drone manufacturers and end users.

1. Provisions Focused on Developers and Manufacturers

An effective new regulatory scheme must focus on privacy practices of drone developers and manufacturers because the risk of individual hackers will be lower if drone developers comply with strict regulatory standards that require encryption or other protections. As an initial matter, to effectively regulate drone manufacturers, the FAA should develop a tiered system for drones based on their size and capabilities. Weighted values should be assigned to different variables that are considered, with more weight placed on the variables most closely correlated with potential privacy threats, such as data acquisition ability, data storage capacity, and flight range. Based on the weighted average of these variables, which should be unambiguous to drone developers, each new drone developed would fall into a single risk category. The minimum-security standards for new drones would then be assigned based on risk category. Once published, this risk scale should enable drone developers and manufacturers to clearly understand the regulatory standards applicable to their aircrafts. These standards might include limitations on the amount of data drones are authorized to store, restrictions on the types of data drones may collect, and the types of disclosure drone operators are required to provide.

---

[148] *Id.*

[149] *S. 631: Drone Aircraft Privacy and Transparency Act of 2017*, GOVTRACK, https://www.govtrack.us/congress/bills/115/s631 [https://perma.cc/DC4F-SB4L].

The vulnerability of civilian drones to hackers and the potentially large quantities of private data that could be misappropriated as a result underscore the need for a regulatory provision requiring drone developers to install antihacking security software. In 2014, the research arm of the Pentagon revealed that it had built a drone equipped with software called High Assurance Cyber Military Systems, a program that protects the drone against all forms of cyber attack.[150]

While such impenetrable software likely will not be commercially available for use in civilian drones in the near future, software has been privately developed that can drastically reduce the risk of hacking by preventing the most common types of attacks.[151] A video posted online by Galois—a new technology research and development company—illustrated the functionality of such software by demonstrating how easily an ordinary drone can be hacked and then demonstrating the inability of the same hacking techniques to gain control of a comparable drone with Galois software installed.[152] Such software could drastically reduce the threat posed by drone hackers, as it would thwart all but the most skilled hackers and consequently, protect the data of millions of Americans. Mandatory antihacking software legislation would be a novel concept but not wholly unheard of; there have been other federal cybersecurity laws passed recently, such as the Cybersecurity Act of 2015[153] that highlight the U.S. government's recognition of the importance of the issue.

In addition to an antihacking software installation requirement, the FAA's drone regulations should mandate that manufacturers and developers include provisions limiting the amount of data that any particular drone can store and the types of data it can acquire. These limitations should be largely based on the intended functionality of different drone models, restricting data collection that falls outside the scope of the drone's intended use, and capping data storage volume based on industry benchmarks. Additionally, as mentioned by EPIC

---

[150] *See* Kris Osborn, *DARPA Unveils Hack-Proof Drone*, DEFENSE TECH (May 21, 2014), https://www.defensetech.org/2014/05/21/darpa-unveils-hack-proof-drone/ [https://perma.cc/7ASF-XN96].

[151] *See* Betsy Lillian, *Galois Develops Anti-hacking Software for Commercial UAVs*, UNMANNED AERIAL ONLINE (Mar. 9, 2015), http://unmanned-aerial.com/galois-develops-anti-hacking-software-for-commercial-uavs/ [https://perma.cc/JZ5Q-X5EZ].

[152] Galois, Inc., *Quadcopter Vulnerabilities and "Hack-Proof" UAV Software*, YOUTUBE (Mar. 18, 2015), https://www.youtube.com/watch?feature=player_embedded&v=uMB10QCxudY.

[153] *See* Consolidated Appropriations Act of 2016, Pub. L. No. 114-113, div. N, 129 Stat. 2242, 2935 (2015).

in its public comment to the FAA, there should be a time limit placed on a drone's data retention so that data is not stored longer than necessary to serve its purpose.[154] Provisions covering drone manufacturers are only a starting point—to comprehensively protect the privacy interests of millions of Americans, the FAA's revised regulations will need to cover drone operators as well.

2. Provisions Focused on End Users

In addition to provisions that target manufacturers, the regulations should include comprehensive regulatory provisions focused on regulating the conduct of end users and potential drone hackers. These provisions will require a balancing of interests including a consideration of existing state privacy laws and First Amendment protections. There are certain provisions for which the consistency of the federal law is indisputably necessary including strict antihacking provisions and an absolute ban on flying drones near private residences or in certain areas where sensitive information is stored ("no fly zones").

Turning first to provisions targeting end users, flying within a specified proximity above or near private residences should be expressly forbidden to prevent unauthorized data collection. Prohibiting drone users from obtaining sensitive data would, in turn, reduce the exposure of this data to potential hackers. Without such a prohibition, there will undoubtedly be an increase in self-help, such as that exemplified by a Kentucky man who recently shot down a drone that was recording video near his residence.[155] Alternatively, consumers can avoid this type of self-help through the use of residential geofencing, which creates a virtual wall around certain pre-set geographic boundaries using GPS technology.[156] One drone company, DJI, has developed an innovative mechanism that would help facilitate this prohibition—an application that shows drone operators restricted areas surrounded by geofencing in real time.[157]

In addition to protecting against residential privacy violations, the FAA's regulations should expand the number of prohibited airspace locations listed by the federal government,

---

[154] *See* EPIC Comments, *supra* note 7, at 15.

[155] *See* Mike Wehner, *Kentucky Man Shoots Down Drone Spying on 16-Year-Old Daughter*, DAILY DOT (July 30, 2015), http://www.dailydot.com/technology/kentucky-drone-shooting/ [https://perma.cc/V9RC-G9BN].

[156] *See* Jason Fitzpatrick, *What Is "Geofencing"?*, HOW-TO-GEEK (July 1, 2015), http://www.howtogeek.com/221077/htg-explains-what-geofencing-is-and-why-you-should-be-using-it [https://perma.cc/LDV5-2P95].

[157] *See DJI Introduces New Geofencing System for Its Drones*, DJI (Nov. 18, 2015), http://www.dji.com/newsroom/news/dji-fly-safe-system [https://perma.cc/R9AX-LF6C].

to ensure the protection of private information. The FAA already prohibits the use of airspace above certain locations across the United States, such as the airspace surrounding significant government buildings and financial institutions,[158] but vastly increasing the size of this list specifically for drones would be an important measure to prevent the capture of confidential information that could pose a threat to our nation's security. In any event, provisions covering end users would be an important component of any regulatory regime that would effectively protect against the unique privacy threats presented by civilian drones.

It will also be important for new regulations to focus on the harmful actors, drone hackers. Just as thieves choose to steal despite it being a criminal act, there will inevitably be malicious individuals who attempt to hack into drones and steal information, regardless of the penalty for the offense. Although it may not impede those who are averse to the law, a strict antihacking provision would serve as a necessary deterrent for the ordinary hobbyist. Of course, the penalties will vary wildly with the magnitude of the offense and the significance of any misappropriated data, but must be severe enough to send a clear message. The sentencing regime for drone hacking should be modeled after existing statutes, such as the Computer Fraud and Abuse Act (CFAA).[159] As with most crimes, repeat offenders should face an enhanced sentence, which could be based on a multitude of circumstances including the intent behind the attack, any property damage caused, or the volume of data stolen. For example, the CFAA provides for a maximum sentence of one-year imprisonment for a first-time computer hacker who obtains financial records, information from a United States agency, or information from a protected computer, but a maximum sentence of five-years for a first-time offender who commits fraud for financial gain of more than $5000.[160]

While a strict sentencing regime should undoubtedly be imposed to effectively deter civilian drone hacking, individual circumstances will inevitably require significant sentencing variance. Absent a strong deterrent, the relative simplicity of hacking into a drone's GPS system using the spoofing technique would likely make it attractive for experimentation to many curious minds.

---

158 *TFR List*, FED. AVIATION ADMIN., http://tfr.faa.gov/tfr2/list.html [https://perma.cc/7Y86-BX6D].

159 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

160 *Id.* § (c)(2)(A), (c)(3)(A).

CONCLUSION

With the age of civilian drones now upon us, the only certainty is that change is unavoidable. Technological change of this magnitude has the potential to foster significant societal development if the United States adequately prepares for it by taking a proactive regulatory approach.

With their lack of privacy protections, existing drone regulations have left a dangerous void in United States law that could lead to privacy invasions and security threats on an unprecedented scale. The privacy threats presented by civilian drones are multifaceted and largely stem from their advanced technological capabilities, their proliferation under the new regulatory regime, and their vulnerability to hackers. To effectively reduce these threats, Congress must act quickly to mandate that the FAA regulate drone privacy. Then, under a new congressional mandate, the FAA must consider the input of many affected stakeholders in issuing comprehensive civilian drone privacy regulations. Absent such legal intervention, many of the negative consequences will inevitably become a reality. By developing comprehensive privacy protections at a federal level, the United States government can avoid stumbling out of the gate, and instead, embrace this impending wave of innovation.

Sean M. Nolan[†]

---

† J.D. Candidate, Brooklyn Law School, 2017; B.S., The University of Tampa, 2012. Thank you to Jessica Schneider, Valentina Lumaj, Alexandra Troiano, Tom McCartin, Christopher Mull, and the entire staff of *Brooklyn Law Review* for their hard work and help preparing this note for publication. I would especially like to thank my girlfriend, Jamie Tynes, and my entire family, for supporting me throughout my endeavor to attain a legal education.