What Is the Eye in the Sky Actually Looking at and Who is Controlling It? An International Comparative Analysis on How to Fill the Cybersecurity and Privacy Gaps to Strengthen Existing U.S. Drone Laws

Jennifer Urban *

TABLE OF CONTENTS

* Jennifer Urban is an Associate in the Charleston, South Carolina office of K&L Gates. Ms. Urban would like to thank Jacqueline Serrao for her helpful insights and Ann Urban for her endless support.

> Recent years have proved such a splendid success for aeronautics that it really seems justifiable for law to begin to take its share in the aerial labour.
>
> - Johanna Francina Lycklama À Nijeholt.[1]

I. INTRODUCTION

Drones are no longer seen as toys only techies get as Christmas gifts;[2] nor are they seen as only being used in new military operations; drones are becoming an integral part of today's global society. UAVs are being used for many different purposes ranging from the National Aeronautics and Space Administration's ("NASA's") use of a drone to collect data and monitor Hurricane Matthew,[3] to construction companies use of drones to map out and supervise large construction projects in order to cut their labor time from months down to minutes.[4]

While UAVs are making many things easier, the benefits come with unique challenges. For example, over the last two years, Dubai International Airport ("DXB") had to shut down three times due to unauthorized drone activity.[5] Each time DXB shut down, it caused a loss of approximately $1,007,310 USD per minute,[6] meaning the shut down on September 28, 2016, for twenty-seven minutes cost Dubai's economy $27,197,370 USD.[7] These shut downs prompted the United Arab Emirates General Civil Aviation Authority ("GCAA") to make DXB a no-fly zone, illustrating the immediate need for drone regulations globally. After these shut downs occurred, Emirates airline asked the GCAA and Dubai Civil Aviation Authority ("Dubai CAA") to enact stricter regulations regarding drone operations around DXB in order to improve the safety of manned aircraft flights

---

1. *See* DONNA A. DUOLO, UNMANED AIRCRAFT IN THE NATIONAL AIRSPACE 3 (Donna A. Dulo, ed., 2015) (citing JOHANNA FRANCINA LYCKLAMA À NIJEHOLT, AIR SOVEREIGNTY 4 (1910)).

2. Many different terms are used to described drones, such as "unmanned aerial vehicles" (UAV), "unmanned aircraft systems" (UAS), and "remotely piloted aircraft" (RPA). These terms will be used interchangeably throughout this paper and each will be discussed in more depth.

3. *See* Alyssa Newcomb, *NASA Deployed This Whale-Shaped Drone to Monitor the Hurricane*, NBC NEWS (Oct. 7, 2016, 1:50 PM), http://www.nbcnews.com/tech/tech-news/nasa-deployed-whale-shaped-drone-monitor-hurricane-n661931 [https://perma.cc/QS3B-XR88].

4. *See* Julian Mitchell, *This Startup Uses Self-Flying Drones to Map and Manage Construction Sites*, FORBES (Sept. 27, 2016, 6:33 PM), https://perma.cc/BB59-F5SRhttp://www.forbes.com/sites/julianmitchell/2016/09/27/this-startup-uses-drones-to-map-and-manage-massive-construction-projects/#7480a81f4334.

5. *See* Sarah Townsend, *Drone Prompts Shutdown at Dubai International Airport*, ARABIAN BUS. PUB. LIMITED (Sept. 28, 2016, 10:17 AM), http://www.arabianbusiness.com/drone-prompts-shutdown-at-dubai-international-airport-647000.html#.V_lrd9x1ZR0 [https://perma.cc/JHD6-8ETG].

6. Approximately AED 3.7 million.

7. *See* Townsend, *supra* note 5.

departing from and arriving at DXB.[8] Due to the difficult nature of identifying the drone operator, it has proven to be challenging to enforce UAS no-fly zones.[9] In order to better enforce the UAS no-fly zone around DXB, the Dubai CAA has begun experimenting with a "drone-hunting" drone that can identify unlawful drone operations within the zone.[10] According to UAS attorneys Jennifer E. Trock and Chris Leuchten, "[t]he drone-hunter aerially patrols the airport perimeter, using a thermal and infrared imaging to detect unauthorized drones, tracks their frequencies, follows the UAS back to its owner, and sends a signal to the Dubai police."[11] The "drone-hunting" drone is one solution posed thus far to help solve unauthorized drone operations and could be helpful in protecting the privacy of ordinary citizens.[12]

Drones violating air space is not the only problem this new technology creates. Both cybersecurity and privacy issues arise as a result of drone activities. A research team at the University of Texas at Austin employed "spoofing"[13] to hack a drone belonging to the university.[14] The spoofing was done through a mechanism where the hackers were able to get the drone to mistake their signals for the ones sent by the owner's GPS satellites.[15] This hack was done for research on drone vulnerability, which confirmed the fear that it is not very difficult for a drone to be hacked and the realization that many cybersecurity implications that could come from this.

The privacy issue related to drones arose in a 2015 lawsuit where David Boggs, a resident of Kentucky, had his drone shot down by his neighbor William Merideth.[16] Merideth argued that the drone operations caused a trespass on his right to privacy.[17] On the opposing side, Boggs argued that, according to title 49, section 40103 of the U.S. Code, "the United States Government has exclusive sovereignty of airspace of the United States," and therefore, Merideth did not own the airspace, so no trespass could have

8. *See* Jennifer E. Trock & Chris Leuchten, *Dubai Airport's New Guardian: a Drone-Hunting Drone*, PILLSBURY: UAS L. BLOG (Dec. 22, 2016), http://www.uaslawblog.com/2016/12/22/dubai-airports-new-guardian-drone-hunting-drone/ [https://perma.cc/SP9T-Z46H].

9. *Id*.

10. *Id*.

11. *Id*.

12. *Id*.

13. Spoofing is defined as "sending a network packet that appears to come from a source other than its actual source. [It] involves – 1) the ability to receive a message by masquerading as the legitimate receiving destination, or 2) masquerading as the sending machine and sending a message to a destination." RICHARD KISSEL, NAT'L INST. OF STANDARDS & TECH., GLOSSARY OF KEY INFORMATION SECURITY TERMS 188 (2013), http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [https://perma.cc/9WK2-JTU6].

14. See *Researchers Use Spoofing to 'Hack' Into a Flying Drone*, BBC NEWS (June 29, 2012), http://www.bbc.com/news/technology-18643134 [https://perma.cc/P368-T4PJ].

15. *Id.*

16. *See* Cyrus Farivar, *After Neighbor Shot Down His Drone, Kentucky Man Files Federal Lawsuit*, ARS TECHNICA (Jan. 6, 2016, 4:00 AM), http://arstechnica.com/tech-policy/2016/01/man-whose-drone-was-shot-down-sues-shotgun-wielding-neighbor-for-1500/ [https://perma.cc/JB7E-F6YS].

17. *Id*.

occurred.[18] There is a lack of precedent on this issue. The most recent case on point is *United States v. Causby* in 1946, where the United States Supreme Court held that a landowner's property rights extended up to 83 feet above his land into the air space.[19] Although this case is relatively on point, it is outdated. It is unlikely the justices in 1946 could have imagined the holding's implications on drones decades later.

Another theory that has been argued is the common law rule of *Cujus Est Solum, Ejus Est Usque Ad Ccelum Et Ad Inferos*, which is defined as "[t]o whomever the soil belongs, he owns also to the sky and to the depths. The owner of a piece of land owns everything above and below it to an indefinite extent."[20] Therefore, if a drone trespasses in air space, it will depend on how high the drone is flying as to whose air space it is violating. Also, this raises the following question: if drones are always violating either a third party's or the government's air space, then where can drones legally fly, besides right above the drone operator's own property? Boggs' lawyer, James Mackler, noted that an important precedent could be set by this case when he stated, "[p]roperty owners deserve to be free from harassment and invasion of their privacy . . . Likewise, aircraft operators need to know the boundaries in which they can legally operate without risk of being shot down. This lawsuit will give clarity to everyone."[21] In a press release, the Federal Aviation Administration ("FAA") clarified that the assumption that airspace below 400 feet is not controlled by the FAA, was false.[22] The FAA further stated that, "[t]he FAA is responsible for the safety of U.S. airspace from the ground up. This misperception [about the FAA's jurisdiction over airspace below 400 feet] may originate with the idea that manned aircraft generally must stay at least 500 feet above the ground."[23] Both cybersecurity issues and privacy issues relating to drones exemplify the lack of laws and solutions on how to handle UAS flights.

This paper will argue that it is imperative for regulations on UAVs to address cybersecurity and privacy issues in order to remain on the forefront of technology within the aviation industry. Although it may seem like it is more important to establish basic laws on UAS usage, legislators need to work proactively, rather than retroactively, to prevent detrimental cybersecurity and invasions of privacy from occurring.

---

18. 49 U.S.C. §40103 (1994).

19. *See generally* United States v. Causby, 328 U.S. 256 (1062).

20. *Cujus Est Solum, Ejus Est Usque Ad Coelum Et Ad Inferos*, BLACK'S LAW DICTIONARY FREE (2nd. ed.), http://thelawdictionary.org/cujus-est-solum-ejus-est-usque-ad-ccelum-et-ad-inferos/ [https://perma.cc/N7H7-4EXT]; Farivar, *supra* note 16.

21. *See* Farivar, *supra* note 16.

22. *See Busting Myths About the FAA and Unmanned Aircraft,* FAA (Feb. 26, 2014), https://www.faa.gov/news/updates/?newsId=76240 [https://perma.cc/R22B-PDRY].

23. *Id*.

II. TECHNOLOGICAL EXPLANATIONS

The definition of "unmanned aircraft" is "an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft."[24] Hot air balloons are likely the first unmanned aircraft; however, they are not always considered as such because the pilot cannot fully control the balloon's flight operations.[25] Further, the term "unmanned aircraft system" means "an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system."[26] A small unmanned aircraft is "an unmanned aircraft weighing less than 55 pounds."[27] The small unmanned aircraft is what the newly enacted Part 107 regulates, which will be discussed later in this paper.[28]

The International Telecommunication Union defines cybersecurity as:

> the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise… availability, integrity, … [and] confidentiality.[29]

According to the United States National Academy of Sciences, cyber attacks are defined as the "deliberate actions to alter, disrupt, deceive,

---

24. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331, 126 Stat. 11, 72 (2012).

25. *See* THE FUTURE OF DRONE USE: OPPORTUNITIES AND THREATS FROM ETHICAL AND LEGAL PERSPECTIVES 9 (Bart Custers ed. 2016); Tom Harris, *How Hot Air Balloons Work*, HOW STUFF WORKS, http://science.howstuffworks.com/transport/flight/modern/hot-air-balloon2.htm [https://perma.cc/U65B-MXRF] (last visited Dec. 26, 2016).

26. FAA Modernization and Reform Act § [?].

27. *Id*.

28. *See* Mary Ellen Callahan & Laura Fong, *FAA final rule doesn't advance drone debate*, L.A. DAILY JOURNAL, (June 29, 2016), https://www.americanbar.org/content/dam/aba/images/air_space/course/16-annual/am16-3-faa-final-rule-drone.pdf [https://perma.cc/2382-NXR6].

29. *Definition of Cybersecurity*, INT'L TELECOMM. UNION, http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [https://perma.cc/QY2H-GZTX] (last visited Dec. 27, 2016).

degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[30]

III. HISTORY OF BASIC DRONE LAW

The United States' airspace is the busiest in the entire world;[31] yet, the government has not provided adequate solutions on how to handle drones and its operations within US airspace. In February 2007, the FAA released a statement that UAS are aircrafts and, as such, the FAA banned commercial drone operations unless the drone operator was given an exemption and was a licensed pilot.[32] The exemptions for commercial operations were to be reviewed by the FAA on a case-by-case basis.[33]

In 2012, Congress enacted the FAA Modernization and Reform Act, which required that the FAA establish regulations to bring UAS into the overall national airspace system.[34] The new FAA regulations had to be established by September 30, 2015.[35] The FAA missed the deadline for enacting regulations regarding drones, claiming that their number one goal was safety and that the enactment of these regulations would take additional time.[36] Thus, litigation ensured.

The Federal Aviation Administration v. Raphael Pirker was the first case in which the FAA fined a drone operator.[37] On October 17, 2011, Pirker used a Zephyr drone to take aerial photographs of the University of Virginia.[38] Due in part to Pirker's use of the drone for commercial purposes without FAA approval, he was charged with operating a drone in a reckless manner and was fined $10,000.[39] The FAA claimed that "Pirker operated the aircraft within about 50 feet of numerous individuals, about 20 feet of a crowded street, and

30. Jennifer Ann Urban, *Not Your Granddady's Aviation Industry: The Need To Implement Cybersecurity Standards and Best Practices Within the International Aviation Industry*, __ ALB L.J. SCI. & TECH. __, (forthcoming 2017) (quoting NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (William A. Owens et al. eds., 2009).

31. *See* Naveen C. Rao, *Federal Regulation of Airspace and Air Traffic*, *in* AVIATION REGULATION IN THE UNITED STATES 333 (David Heffernan & Brent Connor eds., 2014).

32. *See From A Drone's Eye*, CONCORD ACAD. (Nov. 8, 2016), https://concordacademy.org/news/drones-eye-view/ [https://perma.cc/T867-YTWP].

33. *Id*.

34. *See generally*, FAA Modernization and Reform Act § [?].

35. *Id.*

36. *See* Keith Wagstaff, *FAA Misses Deadline for Creating Drone Regulations*, NBC NEWS (Oct. 1, 2015, 3:29 PM), http://www.nbcnews.com/tech/innovation/faa-misses-deadline-creating-drone-regulations-n437016 [https://perma.cc/5NR3-ENVW].

37. *See* Stephen Pope, *FAA Settles Landmark Pirker UAV Case*, FLYING MAG. (Jan. 27, 2015), http://www.flyingmag.com/news/faa-settles-landmark-pirker-uav-case [https://perma.cc/6ZG3-2GNR].

38. *Id*.; *See also* Mike M. Ahlers, *Pilot Wins Case Against FAA Over Commercial Drone Flight*, CNN (Mar. 6, 2014, 10:07 PM), http://www.cnn.com/2014/03/06/us/drone-pilot-case-faa/ [https://perma.cc/TWV5-2F8M].

39. *Id.*

within approximately 100 feet of an active heliport at UVA."[40] When Pirker challenged the $10,000 fine, he initially won and Administrative Law Judge Patrick G. Geraghty dismissed the fine, ruling that model aircrafts were not aircrafts and therefore, not covered by the FAA's commercial aircraft operations regulations.[41] The FAA appealed to the National Transportation Safety Board ("NTSB"), which appointed a new judge who subsequently overturned the initial decision and found that the FAA did have the authority to regulate drones because drones fell within the definition of "aircraft."[42] Due to the FAA's win on appeal, the original $10,000 fine was re-imposed.[43] The FAA and Pirker finally reached a settlement in January 2015.[44] The settlement allowed Pirker to not admit guilt and dropped the fine to $1,100.[45] A key takeaway from this case is that it portrayed the need for clear regulations on drone operations.

The FAA separated its regulations of UAS based on the type of operation of the drone, as well as its specific characteristics, such as size and power.[46] On December 21, 2015, the FAA's first regulations regarding recreational use of drones went into effect.[47] One of the key regulations enacted requires owners of a drone weighing between 0.55 and 55 pounds to register the drone with the FAA before it legally can be operated.[48] After the recreational owner registers the drone, it must abide by the following FAA safety guidelines:

- "Fly at or below 400 feet;
- Be aware of airspace requirements and restrictions;
- Stay away from surrounding obstacles;
- Keep your UAS within sight;
- Never fly near other aircraft, especially near airports;
- Never fly over groups of people;
- Never fly over stadiums or sports events;

40. *Id*.
41. *Id*.
42. *See* David Esler, *FAA vs. Raphael Pirker*, AVIATION WK. NETWORK (Dec. 28, 2015), http://aviationweek.com/bca/faa-vs-raphael-pirker [https://perma.cc/4QF6-LS69].
43. *Id*.
44. *Id*.
45. *Id*.
46. *See generally* FAA Modernization and Reform Act § [?].
47. *See From A Drone's Eye*, CONCORD ACAD. (Nov. 8, 2016), https://concordacademy.org/news/drones-eye-view/ [https://perma.cc/RR8U-8K6K]; The recreational use of small unmanned aircraft systems ("UAS") is the operation of an unmanned aircraft for personal interests and enjoyment. For example, using a sUAS to take photographs for your own personal use would be considered recreational; using the same device to take photographs or videos for compensation or sale to another individual would be considered a commercial operation. *See Recreational Users*, KNOW BEFORE YOU FLY, http://knowbeforeyoufly.org/for-recreational-users/ [https://perma.cc/5PFT-MYTU] (last visited Dec. 28, 2016).
48. *See* Registration and Marking Requirements for Small Unmanned Aircraft, 80 Fed. Reg. 78593 (Dec. 21, 2015).

- Never fly near emergency response efforts such as fires; [and]
- Never fly under the influence of drugs or alcohol."[49]

Before the new commercial use of small drone regulations went into effect in 2016, there were three specific ways to partake in commercial UAS operations.[50] The three options were:

> (i) apply for and obtain an exemption from the supervision and registration requirements of the Federal Aviation Act pursuant to Section 333 of the FAA Modernization and Reform Act of 2012 (Section 333 Exemption) and operate the UASs pursuant to the express terms of the Section 333 Exemption;
> (ii) obtain an airworthiness certificate for the UASs and operate the aircraft by a pilot pursuant to an operating certificate; or
> (iii) obtain a Certificate of Waiver or Authorization from the FAA and operate the UASs pursuant to the terms of such Certificate of Waiver of Authorization.[51]

An Airman Certificate was required by the drone operator under all three of these options.[52] Although most commercial drone usage at that time fell under the Section 333 Exemption, when operations were conducted by public entities it was only necessary to get a Certificate of Waiver/Authorization.[53] The section 333 exemption allowed the Secretary of Transportation to determine, on a case-by-case basis,[54] as to whether individual drone operations could be conducted safely within the United States national airspace.[55] Through the Section 333 petitions reviewed before

49. *Fly for Fun*, FAA, https://www.faa.gov/uas/getting_started/fly_for_fun/ [https://perma.cc/832E-GLZL] (last visited Dec. 28, 2016).

50. *See* Marcelle Lang & Thomas A. Zimmer, *Update: Commercial Drone Operations in the US*, VEDER PRICE PC (Dec. 2016), http://www.vedderprice.com/Update-Commercial-Drone-Operations-in-the-US-12-20-2016/.

51. *Id*.

52. *Id*.

53. *See* Lang & Zimmer, *supra* note 50. A Certificate of Waiver or a Certificate of Authorization is defined as "a Federal Aviation Administration grant of approval for a specific flight operation." FAA Modernization and Reform Act § [?].

54. FAA Modernization and Reform Act of 2012 § 333(b). According to Section 333(b): [i]n making the determination under subsection (a), the Secretary [of Transportation] shall determine, at a minimum – (1) which types of unmanned aircraft systems, if any, as a result of their size, weight, speed, operational capability, proximity to airports and populated areas, and operation within visual line of sight do not create hazard to users of the national airspace system or the public or pose a threat to national security; and (2) whether a certificate of waiver, certificate of authorization, or airworthiness certification . . . is required for the operation of unmanned aircraft systems.

55. *Id*.; *See also* Lang & Zimmer, *supra* note 50.

Part 107 was enacted,[56] the FAA was able to learn from and adjust its original regulations to help create the final regulations in Part 107.[57]

The highly anticipated FAA regulations on small drones were released in June 2016, with a focus on balancing safety and economic factors.[58] These rules are for commercial drone operations, as opposed to recreational flights.[59] According to the FAA, over the next ten years, these new regulations could help create at least an $82 billion increase in the U.S. economy and 100,000 new jobs.[60] Part 107, the non-recreational drone operation regulations, finally went into effect on August 29, 2016, nearly a year after they were supposed to have been enacted.[61] Part 107 rules apply to drones that weigh less than 55 pounds and regulate many different types of commercial operation.[62] One key aspect of Part 107 is that it requires the operator hold a "remote pilot airman certificate with a small UAS rating" or be directly supervised by a person that has earned this certificate.[63] Another important aspect of Part 107 is that, if a planned drone operation does not completely comply with the FAA's regulations, the operator must obtain a waiver before this drone operation can take place.[64] the other Part 107 basic rules for commercial drone operation are similar to the recreational operation rules discussed above and require that the operator:

- operate the Small UASs within visual line of sight of the Remote Pilot;
- operate the Small UASs during daylight hours;
- operate the Small UASs at a height of not more [than 400 feet];
- operate the Small UASs at or below 100 mph;
- not fly the Small UASs over people except for those participating in the operation or those under a covered structure;
- not operate the Small UASs from a moving vehicle unless the operation is over a sparsely populated area;
- yield the Small UASs to manned aircraft; and

56. *See Section 333*, FAA, https://www.faa.gov/uas/beyond_the_basics/section_333/ [https://perma.cc/M5L5-DR2R] (last visited Dec. 28, 2016). As of September 28, 2016, 5,551 petitions had been granted and 1,780 had been closed. *Id.*

57. *See* Lang & Zimmer, *supra* note 50.

58. Callahan & Font, *supra* note 28.

59. *Id*.

60. *Id*.

61. *The FAA's New Drone Rules Are Effective Today*, FAA (Aug. 29, 2016, 12:07 PM EST), https://www.faa.gov/news/updates/?newsId=86305 [https://perma.cc/PCN6-6V3X].

62. *Fact Sheet – Small Unmanned Aircraft Regulations (Part 107)*, FAA (June 21, 2016), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516 [https://perma.cc/K22C-HKR8].

63. *Id.*

64. *Id.*

- only operate the Small UASs in non-FAA controlled airspace.[65]

If the FAA finds that the operations outside Part 107 allowances can be done in a safe manner, it is likely that the FAA will issue the waiver or airspace authorization.[66] As of October 25, 2016, the FAA had denied 71 Part 107 waiver requests and 854 airspace authorization requests.[67] The FAA announced that most of these denials were due to the request having wrong or missing information.[68] Further, the FAA clarified that many of the denied requests were due to applicants trying to receive too many waivers of Part 107 regulations or gain authorization in the types of airspace that the FAA has not yet approved for drone operations.[69] Although Part 107 allows the FAA a flexible model with which to work for commercial drone operations,[70] it does not provide enough clarification on how the issues of privacy and cybersecurity with drones should be handled.

IV. DRONE CYBERSECURITY ISSUES

The potential for cyber attacks may not initially be viewed as a concrete threat to the United States as compared to other security issues, such as bombings and in-person hijackings, but cyber attacks can create just as much damage.[71] According to researchers at the National Research Foundation of Korea, drones are highly susceptible to cybersecurity issues because they have a "highly exposed technical system due to the unique configuration such as open state of the sensors at all times, wireless network, serially safety structure, etc."[72] The three main classifications under which cyber attacks on drones can be categorized are hardware attacks,[73] wireless attacks,[74] and sensor spoofing.[75] Each of these presents new obstacles that must be overcome in order to ensure secure and safe drone operation and require legislators to establish regulations that pertain to each classification. Drone

65. Lang & Zimmer, *supra* note 50.

66. *Id*.

67. *See FAA Issues Part 107 Waivers, Airspace Authorizations*, FAA (Oct. 25, 2016, 9:50 AM EST), https://www.faa.gov/news/updates/?newsId=86707 [https://perma.cc/57S6-2U2J].

68. *Id*.

69. *Id*.

70. *Id*.

71. *See* Urban, *supra* note 30, at 64.

72. Young Sil Lee et al., *An Overview of Unmanned Aerial Vehicle: Cyber Security Perspective*, 4 ASIA-PACIFIC PROCEEDINGS OF APPLIED SCI. & ENG'G FOR BETTER HUMAN LIFE 128, 129 (2016).

73. Hardware attacks occur when the "attacker has access to the UAV autopilot components directly." *Id*. at 130.

74. Wireless attacks occur when the "attacker carries out the attacks through one of the wireless communication channels." *Id*.

75. Sensor spoofing is occurs when the "attacker passes false data throughout the on-board sensors (e.g., GPS receivers, vision, radar, sonar, LIDAR, and the IR sensors) of the UAV autopilot." *Id*.

cybersecurity issues are a great context within which the government can be proactive rather than reactive in developing its regulations, if substantial work begins immediately. While discussing the difficulty of keeping cybersecurity standards up-to-date with technological advances, Axel Jahn, the managing director of vice president of business development for connectivity at TriaGnoSys, stated, "[w]hat has been established is going to be outdated as soon as you publish it so we maybe need to have a new philosophy on how we are installing things in an aircraft."[76] In this regard, it is imperative that any new regulatory measures be flexible enough to advance a technology as drones advance.[77] Cybersecurity solutions are currently emphasized in aviation,[78] so it makes sense to continue on this path to include UAS in the aviation sector, which needs guidance for these types of potential risks.

In its commentary on the new FAA regulations on UAS, the Electronic Privacy Information Center ("EPIC") stated that "[t]he integration of drones into the NAS ["National Airspace System"] will mean that thousands of new, hackable devices will be hovering over our homes and streets without any clear security guidance, despite known vulnerabilities."[79] Drone operations can be hacked and its stored information could then be intercepted and compromised, creating both a security problem and a privacy issue.[80] In October 2016, the United States Federal Trade Commission ("FTC") illustrated how easily drones can suffer cybersecurity issues when it hacked into three different types of drones sold to civilians, which cost the FTC less than $200 to do so.[81] The FTC hacks also portrayed how easily an operator's and a third-party's privacy rights could be violated by a hacker.[82] According to the FTC, these are the four main points demonstrated by the hacks:

- Researchers were able to take over the video feed on all three of the drones, since the data was sent unencrypted.
- With two of the drones, they were able to take control of the flight path, as well as turn off the aircraft, causing both to fall from the sky.
- All of the smartphone apps made for the devices gave no indication or inconsistent notifications when a third party

76. Juliet Van Wagenen, *Experts Speak to Cyber Security in* Aviation, AVIONICS TODAY (June 12, 2015), http://www.aviationtoday.com/av/topstories/Experts-Speak-to-Cyber-Security-in-Aviation_85266.html [https://perma.cc/SH6Q-A9T9].

77. *Id*.

78. Urban, *supra* note 30, at 64.

79. Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. §§ 21, 43, 61, 91, 101, 107, 119, 183 (2016)

80. *See* Amie Stepanovich, *Legal Safeguards Are Needed to Protect Against Domestic Use of Drones*, *in* DRONES 100, 103 (Louise Gerdes ed., 2014).

81. *See* 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, 5:07 PM), http://www.recode.net/2017/1/4/14062654/drones-hacking-security-ftc-parrot-dbpower-cheerson [https://perma.cc/YWW6-V45D].

82. *Id*.

was connecting to the drone, so the operator wouldn't know if someone was watching the video feed.

- Each of the drones acted as a Wi-Fi access point, allowing devices to connect to the drone like a home router, but, according to the FTC, they required no password to actually connect.[83]

The FTC stated that UAS manufacturers can tighten drone security and prevent successful cyber attacks on drones by encrypting the UAS with a wi-fi signal that is password protected.[84] This hacking lesson is a perfect demonstration of drone cybersecurity issues and provides ways UAS operators can prevent or limit these types of issues from occurring. The United States Government should keep taking actions similar to those of the FTC in order to continue the development of drone cybersecurity solutions in areas where these issues can be regulated.

On December 27, 2016, then President-elect Donald Trump announced that Thomas P. Bossert would serve as assistant to the president for homeland security and counterterrorism.[85] In this position, Bossert would be responsible for addressing cybersecurity issues.[86] When discussing his appointment of Bossert, President-elect Trump stated, "[h]e has a handle on the complexity of homeland security, counterterrorism and cybersecurity challenges."[87] In response to his appointment, Bossert said that the country:

> [M]ust work toward [a] cyber doctrine that reflects the wisdom of free markets, private competition and the important but limited role of government in establishing and enforcing the rule of law, honoring the rights of personal property, the benefits of free and fair trade and the fundamental principles of liberty.[88]

The statements released around this appointment by both President-elect Trump and Bossert do not give the impression that there will be substantial cybersecurity policy changes by the new administration, but only time will tell how cybersecurity issues are addressed.[89] Bossert has the ability to address and help solve a vast array of cybersecurity issues' hopefully, one of which will be cybersecurity surrounding drones. In turn with his free market stance, Bossert could possibly use his position to bring together different industry members to help solve drone cybersecurity threats without

83. *Id*.
84. *Id*.
85. *See* Michael D. Shear, *Trump Picks Thomas Bossert as Top Counterterrorism Adviser*, N.Y. TIMES (Dec. 27, 2016), http://www.nytimes.com/2016/12/27/us/politics/thomas-bossert-national-security-trump.html?_r=0 [https://perma.cc/B8T5-3YFW].
86. *Id*.
87. *Id*.
88. *See* Jimmy H. Koo, *Trump Names Cybersecurity Adviser with Free Markets View*, BLOOMBERG (Dec. 29, 2016), https://www.bna.com/trump-names-cybersecurity-n73014449113/ [https://perma.cc/92ES-2ZHG].
89. *Id*.

the need for only government legislators being involved. It is imperative that all members of the international UAS community help develop, implement, and follow cybersecurity frameworks and measures in order to maintain safety throughout the entire UAS industry and all drone operations.

Another cybersecurity issue that has recently arisen is in the market for drone-countering technologies.[90] The purpose of drone-countering technology is to stop drones from operating where they should not be flying or from conducting intrusive activities.[91] Although non-governmental use of these technologies is outlawed in the United States due to drones being private property, there is still a chance they will be used illegally.[92] Recently, the FAA has been testing drone-countering technologies at Denver International Airport.[93] The technologies being tested range from services that detect UAS around airports and "geofencing software," that could potentially be required on non-government operated drones, to automatically prevent drones from flying in certain areas.[94] This testing is authorized under and funded by the Fiscal Year 2016 appropriations regulations, which require the FAA look into drone-countering technologies, and the FAA Extension, Safety and Security Act, which allowed for $6,000,000 to be spent on "airspace hazard mitigation at airports and other critical infrastructure using unmanned aircraft detection systems."[95] The FAA's goal is to have set drone-countering technologies that will be used at airports by the Fall of 2017.[96]

These new drone-countering technologies are working on "cracking the radio wireless protocols used to control a drone's direction and payload to then take it over and block its video transmission."[97] For example, DroneVision Inc. of Taiwan claims that it is the first drone-countering company that is able to "anticipate the frequency hopping that many drones use . . . " [and] "the anti-drone gun – resembling a rifle with two oversized barrels, coupled with a backpack – blocks the drone's GPS signals and video transmission, forcing it to return to where it took off via the drone's own failsafe features."[98] The argument for drone-countering technologies is that they allow people to stop drone operations from infringing on their privacy rights.[99] Non-governmental use of drone-countering technologies creates a huge cybersecurity problem and many safety issues.

One reason for the development of drone-countering technologies is the lack of regulations protecting a person's privacy from drone operations. The

---

90. *See* Jeremy Wagstaff & Swati Pandey, *Dog Fight: Start-ups Take Aim at Errant Drones*, REUTERS (Jan 2, 2017, 8:29 PM), http://www.reuters.com/article/us-tech-drones-idUSKBN14M180 [https://perma.cc/Q8LV-C6TX].

91. *Id*.

92. *Id*.

93. *See* Bill Carey, *FAA Will Evaluate 'Counter-UAS' Technology at Denver Airport*, AIN (Nov. 9, 2016, 10:53 PM), http://www.ainonline.com/aviation-news/aerospace/2016-11-09/faa-will-evaluate-counter-uas-technology-denver-airport [https://perma.cc/KY9B-S49N].

94. *Id*.

95. *Id*.

96. *Id*.

97. *See* Wagstaff & Pandey, *supra* note 90.

98. *Id*.

99. *Id*.

lack of drone cybersecurity regulations across the world allows the public to try and take on the issue by themselves. Cybersecurity issues pose a risk to safety, making them fall under the purview of the FAA, therefore, the FAA quickly needs to determine how best to regulate and solve the existing and future problems that come with drones. It is critical to regulate how cybersecurity technologies can and cannot be used by the public to interfere with drone operations.

V. DRONE PRIVACY ISSUES

Privacy law is defined as "[r]egulation[s] or statute[s] that protect a person's right to be left alone, and govern collection, storage, and release of his or her financial, medical, and other personal information."[100] In regards to technology as a whole, most privacy laws are outdated.[101] For example, the United States government has not updated or clarified privacy laws regarding technology devices, such as Fitbit, which as of right now are likely much more widely used than drones.[102] Although a Fitbit could allow for infringement on the user's privacy and a drone would allow for a drone user to infringe on a third-party's privacy rights, both portray the issue of privacy laws not adequately regulating technological devices. When referring to drones, former United States Defense Secretary Robert Gates claimed, "[t]he more we have used them, the more we have identified their potential in a broader and broader set of circumstances," which exemplifies the increasing uses that need to be regulated.[103] The rulemaking body has a difficult task of balancing the needs of security, such as drone surveillance in criminal matters, and not infringing on privacy rights.[104] It is critical that rulemaking bodies prioritize the crafting of new laws to handle the privacy concerns that come with drones.

A. History of Drone Privacy Laws

Many privacy advocates argue that, before more drones are allowed to enter airspace, there needs to be adequate legal safeguards established to protect citizens from drones violating their constitutionally protected privacy.[105] According to EPIC's association litigation counsel, Amie Stepanovich, "[d]rones may … carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers."[106] These

100. *Privacy Law*, BUS. DICTIONARY, http://www.businessdictionary.com/definition/privacy-law.html [https://perma.cc/42LP-T3BQ] (last visited Oct. 6, 2016).

101. *See* Jennifer Ann Urban, *Has GPS Made the Adequate Enforcement of Privacy Laws in the United States a Luxury of the Past?*, 16 J. BUS. L. & INTELL. PROP. L. 400, 414 *(2016).*

102. *Id*. at 402-03.

103. *See* John W. Whitehead, *The Domestic Use of Drones Poses Serious Threats to Civil Liberties*, *in* DRONES 63, 64 (Louise Gerdes ed., 2014).

104. *See generally* COUNTERTERRORISM TECHNOLOGY & PRIVACY 16 (2005).

105. Stepanovich, *supra* note 80, at 100.

106. *Id*. at 101.

capabilities allow for in-depth and constant surveillance, which human surveillance could not provide on the same level.[107] Although this technology continually advances, the laws surrounding it have not followed suit. Currently, there are no sufficient laws in place to protect privacy rights from drone technology and its increasing use in everyday life.[108]

B. General Privacy Laws

The First, Third, Fourth, and Fifth Amendments to the United States Constitution pertain to privacy.[109] The First Amendment gives persons the right to have their own personal, private beliefs.[110] The Third Amendment protects a person's privacy within their home by not allowing soldiers to use a private person's home.[111] The Fourth Amendment protects the privacy of a person in the United States against unlawful search and seizure.[112] The Fifth Amendment protects the privacy of personal information by not requiring a person to commit self-incrimination.[113] None of these four amendments adequately address privacy violations committed by private persons to other persons. While the Fourth Amendment helps solve the privacy issue of government officials potentially using drones to commit unlawful searches, it does not help when a non-governmental entity uses a drone to commit surveillance and violate a person's privacy rights. The public cannot rely on these amendments alone to address privacy risks posed by new technologies, such as drones.

Another place to look for guidance on privacy laws is in Section 652B of the Second Restatement of Torts.[114] This section states "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[115] The standard used by this restatement is that of the reasonable person, which can be difficult to apply to drones.[116] This is because the technology is so new that it may not be possible to determine what a reasonable person would do in a situation.

Two examples may exemplify this issue better. First, if a drone operator was purposefully using his drone to hover over the fenced in pool of his neighbor to record her sunbathing, it is likely that a court would find his actions to be highly offensive to a reasonable person. The neighbor is likely

---

107. *Id*. at 102.

108. *Id*. at 105.

109. *See* Tim Sharp, *Right to Privacy: Constitutional Rights & Privacy Laws*, LIVE SCIENCE (June 12, 2013, 5:34 PM EST), http://www.livescience.com/37398-right-to-privacy.html [https://perma.cc/78V7-TDES], *cited in* Urban, *supra* note 101.

110. *Id*.

111. *Id*. *See also* U.S. CONST. amend III.

112. *See* Urban, *supra* note 101.

113. *Id*. *See also* U.S. CONST. amend. V.

114. *See generally* RESTATMENT (SECOND) OF TORTS § 652 (AM. LAW INST. 1979), https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm.

115. *Id*.

116. *Id*.

to feel as though her private backyard pool no longer remained private and that there had been an invasion of her privacy. Second, if a new drone operator was testing the drone he received for his birthday and intentionally flew it over his neighbor's backyard trying to record a bird, but also accidentally in turn recorded not only the bird, but his sunbathing neighbor, the standard would likely prove to be more difficult to decipher. A reasonable person may not find his action highly offensive since he did not intend to record his neighbor, despite violating herprivate backyard. The reasonable person standard also would require the determination of whether intent was needed for a violation of privacy through drone operations to occur. If the drone operator immediately deletes the recording of his neighbor, since he only wanted pictures of the birds, a reasonable person may be more likely to not find a violation of privacy in this context versus if he purposely wanted to keep or distribute the images of the neighbor. Due to the lack of clarification on how to apply the reasonable person standard to drone operations, tort law does not provide an adequate solution to privacy issues raised by drones.

In his concurrent opinion in *United States. v. Jones*, Justice Alito also used Justice Murphy's quote from *Goldman v. United States*, which perfectly sums up technology's impact on privacy laws, stating:

> the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.[117]

Similar to the analysis of Section 652B of the Second Restatement of Torts, the changes and advancements in technology create gaps in the legal framework because differing perceptions of privacy make it difficult to develop a privacy standard.[118]

Justice Alito further emphasized, in his concurrence in *Jones*, that while people may not like the decrease in privacy that new technologies may create, people may still accept less privacy rights because they see the technologies' diminishment of privacy as unavoidable.[119] In respect to drone operations, it is important that people do not fall into the trap of accepting diminished privacy laws and, instead, push for better privacy legislation to protect their fundamental rights.[120] Without this push, the detrimental consequences of drone operators not having to consider the privacy of others would leave a world where one would have nearly no privacy, unless they were inside a room with no windows so that drone cameras could not see them (at least until drone technologies had the capability to see through walls). Justice Alito

117. United States v. Jones, 132 S. Ct. 945, 959 (2012) (Alito, J., concurring) (quoting Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting)), *cited in* Urban, *supra* note 101.

118. *Id.,cited in* Urban, *supra* note 101, at 424.

119. *Id.*

120. *Id.*

suggested that the best way to handle technology changes and privacy laws is through legislative action.[121] Justice Alito explained that:

> The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements . . . A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.[122]

By developing and enacting new drone privacy laws, the legislature will limit the amount of interpretation that courts will need to do and will help to avoid courts' ruling on these issues with inconsistent interpretations.[123] Although *Jones* was about deciphering global positioning systems' impact on privacy laws, the technological advancement of privacy issues are similar to those created by drones and, at least, provide a bit of direction on the best path to solutions.

C. Drone Specific Privacy Laws

Thus far, the bits and pieces of privacy laws and explanations put into place in the United States cannot be compiled to make a clear or comprehensive privacy law doctrine that can be applied to new technologies within this "cyber age."[124] In 2012, the Association for Unmanned Vehicles Systems International ("AUVSI") established a Code of Conduct for the drone industry.[125] Although the idea was well intentioned, the usefulness of this action was minimal due to the lack of consequences for any violations of the Code.[126] The Code specifically states, "[w]e will respect the privacy of individuals" but it does not give an answer as to what should be done if this privacy is not respected by a drone operator.[127] This Code of Conduct calls on the industry to hold other members to "a high professional and ethical standard," yet it does not have support from the rest of the industry.[128] Even though AUVSI claims it is "serving more than 7,500 members from

121. Stepanovich, *supra* note 80, at 105.

122. *Jones*, 132 S. Ct. at 963–64 (Alito, J., concurring), *cited in* Urban, *supra* note 101, at 425.

123. Urban, *supra* note 101.

124. *See* AMITAI ETZIONI, THE NEW NORMAL 105 (2015).

125. Peter W. Singer & Jeffrey Lin, *A Drone Industry Code of Conduct Is Inadequate to Protect Americans*, *in* DRONES 94, 96–97 (Louise Gerdes ed., 2014); *Unmanned Aircraft System Operations Industry "Code of Conduct"*, ASSOC. FOR UNMANED VEHICLE SYS. INT'L (2012) [hereinafter *Code of Conduct*], http://www.auvsi.org/content/conduct [https://perma.cc/V56B-ZL92].

126. Singer & Lin, *supra* note 125.

127. *Code of Conduct*, *supra* note 125; Singer & Lin, *supra* note 125, at 96–97.

128. *Code of Conduct*, *supra* note 125.

government organizations, industry and academia,"[129] the Code of Conduct only listed seventeen members that supported it.[130] The fact that the Code of Conduct itself mentions how it hopes to gain the support of the entire UAS industry and the small number of listed supporters, solidifies that support from industry members of all sectors is still significantly lacking.[131] Additionally, the Code of Conduct is extremely vague and short. It provides no real guidance or regulation on the operation of drones by any type of user. The Code of Conduct helped initiate the general discussion on privacy and security issues, but lacked actual substance in tackling these problems. Therefore, it is necessary industry members from both the public and private sectors to work together to establish a solution that can significantly handle the large issues of privacy and security in terms of drone usage before the issues get even more out of hand.

Aviation attorney, Mark Dombroff's, prediction that "it is pretty much a 'slam dunk' that Part 107 won't have any privacy rules," was found to be accurate when the new regulations were finally released.[132] The FAA consciously chose not to address critical privacy concerns within Rule 107.[133] EPIC brought suit against the FAA for not addressing privacy issues created by unmanned aircraft, however, the Court rejected EPIC's suit as premature, since the proposed rulemaking had not yet gone into effect.[134] The FAA argued that it is not tasked with addressing privacy concerns and that it is exclusively tasked with "maintaining a safe and efficient national airspace."[135] Instead of tackling these privacy concerns on its own, the FAA explained that it "intend[ed] to continue addressing privacy concerns through engagement and collaboration with the public, stakeholders and other agencies with authority and subject matter expertise in privacy law and policy. Privacy is beyond the purview of its mission of safety and efficiency."[136] Different solutions from around the world as to how these issues should be

129. *See Who is AUVSI?*, ASSOC. FOR UNMANED VEHICLE SYS. INT'L (2012), http://www.auvsi.org/home/learnmore [https://perma.cc/9AYS-KH2E].

130. *Code of Conduct*, *supra* note 125. The members that are listed on the AUVSI website as supporters of the Code of Conduct are: American Aerospace Airborne Systems Group, Arcturus UAV, Aviation Management, CAV Ice Protection, Cochise College, Domaille Engineering LLC, Dragonfly Pictures Inc., FreeWave, INSITU, ISR Group, Kawak Aviation Technologies, Mesa County Sheriff's Office – Colorado, Reactel, Incorporated, Tiffin Technologies, Toyon Research Corporation, UAV MarketSpace, and XRDi. *Id.*

131. *Id.*

132. *See* Mark Dombroff, *UAS/FAA: The FAA Has No Business In The Privacy Business!*, DENTONS: PLANE-LY SPOKEN BLOG (May 26, 2016), http://www.planelyspokenblog.com/uasfaa-the-faa-has-no-business-in-the-privacy-business [https://perma.cc/C2BA-DXQC].

133. Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. §§ 21, 43, 61, 91, 101, 107, 119, 183 (2016).

134. *See generally* Electronic Privacy Info. Ctr v. FAA, 821 F.3d 39 (D.C. Cir. 2016).

135. *See* Bryan Koenig, *FAA Tells D.C. Circ. Drone Privacy Challenge Doesn't Fly*, LAW360 (Nov. 5, 2015, 7:46 PM EST), http://www.law360.com/articles/723976/faa-tells-dc-circ-drone-privacy-challenge-doesn-t-fly [https://perma.cc/6R9L-GEEU].

136. *See* Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. §§ 21, 43, 61, 91, 101, 107, 119, 183 (2016).

regulated, and who is in charge of the regulating, are discussed *infra*. These other nations' regulators vary between courts, legislatures, and government agencies. In order to remain consistent with aviation laws, the overall regulations on drone operations should remain within the purview of the federal government. It would be helpful for Congress to enact additional legislation that addresses privacy issues regarding drones, but guidance from federal agencies could also be useful in quickly creating solutions to these issues.

Part 107's analysis provided by the FAA points interested individuals to the National Telecommunications and Information Administration's ("NTIA's") "Voluntary Best Practice for UAS Privacy, Transparency, and Accountability" ("NTIA Best Practices"), which will be discussed *infra*.[137] Although these Best Practices at least attempt to solve drone privacy issues, its self-regulating and non-binding nature make it unlikely that they will be followed.[138] While the FAA is correct in that privacy falls outside its areas of duty, the unsolved issue of who should be tasked with handling drone privacy concerns continues to hamper the discussion on solutions and delay this time-sensitive issue.[139] As mentioned previously, the best group to address privacy issues, since the FAA is unable, is the United States legislature. The legislature should not be the only entity tasked with solving these issues, though. The entire drone industry should be involved in developing solutions, but the legislature should take the lead.

D. Voluntary Best Practices for UAS Privacy, Transparency, and Accountability

On May 19, 2016, NTIA released a "Best Practices document" encompassing the ways multistakeholder group best addressed the issues of privacy, transparency, and accountability for civilian drone operations, including commercial operations.[140] The NTIA Best Practices suggest guidelines for drone operators to follow.[141] For example, one suggestion is to attempt not to fly over private property.[142] This may sound sensible in theory, but in reality, it is very unlikely to be followed or even plausible.[143] A big problem surrounding the Best Practices is the fact that they are completely

137. Callahan & Fong, *supra* note 28.

138. *Id*.

139. *Id*.

140. The multistakeholder group consisted of "representatives from industry, news organizations, consumer and privacy advocacy groups, academics and trade associations." *NTIA Releases Drone Privacy Best Practices*, HUNTON & WILLIAMS: PRIVACY BLOG (May 20, 2016), https://www.huntonprivacyblog.com/2016/05/20/ntia-releases-drone-privacy-best-practices/ [https://perma.cc/C2J4-K3LJ].

141. Callahan & Fong, *supra* note 28.

142. *Id.*

143. *Id*.

voluntary and no one is actually required to follow them.[144] NTIA makes clear that "[i]n some cases, these Best Practices are meant to go beyond existing law and they do not – and are not meant to – create a legal standard of care by which the activities of any particular UAS operator should be judged."[145]

The five main best practices that NTIA gives are quoted as follows:

1. Inform others of your use of UAS . . .
2. Show care when operating UAS or collecting and storing covered data . . .
3. Limit the use and sharing of covered data . . .
4. Secure covered data . . .
5. Monitor and comply with evolving federal, state, and local laws.[146]

Under Best Practice one, it is recommended that drone operators notify individuals of the approximate timeframe of the operations and that the drone may be purposefully capturing covered data.[147] Under Best Practice two, the drone operator should not purposefully use a UAS to collect covered data where it is reasonable to believe a person in that area has an expectation of privacy.[148] Best Practice three recommends that a drone operator should not use covered data that they have collected from their UAS operations without permission for these purposes: "employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility."[149] Best Practice four suggests that UAS pilots take reasonable steps to handle security threats of covered data by establishing adequate safeguard measures.[150] The Best Practices suggest the following ways of minimizing drone security risks, "appropriate administrative, technical, and physical safeguards include those described in guidance from the Federal Trade Commission, the National Institute of Standards and Technology ("NIST") Cybersecurity Framework, and the International Organization for the Standardization's 27001 standard for information security management."[151]

It is great that the Best Practices address cybersecurity. The solutions they give are on the right track to preventing cybersecurity attacks. These solutions will hopefully lead to regulation in this area and more guidance on

144. *See Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*, NAT'L TELECOMMS. & INFO. ADMIN. (May 19, 2016), https://www.ntia.doc.gov/files/ntia/publications/voluntary_best_practices_for_uas_privacy_transparency_and_accountability_0.pdf [https://perma.cc/2RGC-6W89].

145. *Id.*

146. *Id*. The term "covered data" is defined as "information collected by a UAS that identifies a particular person. If data collected by UAS likely will not be linked to an individual's name or other personally identifiable information, or if the data is altered so that a specific person is not recognizable, it is not covered data." *Id.*

147. *Id.*

148. *Id.*

149. *Id.*

150. *Id*.

151. *Id*.

how to address cybersecurity threats. Finally, Best Practice five makes sure to remind drone operators to stay informed about the changing laws regarding the UAS industry.[152]

There are still many issues that remain unsolved by NTIA's Best Practices. First, it remains unclear how much privacy a person can expect to have on their own property.[153] Due to the advancements in technology, the reasonable expectation of privacy standard has been brought into question.[154] Second, data collection by drones has raised the issue of how legal it is to collect data on other people or activities without permission.[155] This involves the need to regulate the data in many contexts, such as the type of information, its purpose, and its storage.[156] The guidelines do provide some guidance on the data issue, but they are not detailed enough to completely clarify data collection, storage, and distribution with the many different ways in which they can be done. Overall, the Best Practices provide decent guidance on how to prevent some privacy and cybersecurity issues with UAS operations. The multistakeholder approach is the perfect way to get members of all areas of the drone industry involved, but the Best Practices are still a long way from providing critical, concrete, and mandatory solutions to these issues.

VI. GLOBAL DRONE LAWS AND SOLUTIONS

In a 2014 statement, the FAA challenged the notion that commercial drone operations' approval is behind that of other nations.[157] The FAA claimed that:

> The United States has the busiest, most complex airspace in the world, including many general aviation aircraft that we must consider when planning UAS integration, because those same airplanes and small UAS may occupy the same airspace. Developing all the rules and standards we need is a very complex task, and we want to make sure we get it right the first time. We want to strike the right balance of requirements for UAS to help foster growth in an emerging industry with a wide range of potential uses, but also keep all airspace users and people on the ground safe.[158]

The FAA is not solely focused on aviation regulations within the United States, but is tasked with working with other nations to solve joint aviation

152. *Id*.
153. *See* Callahan & Fong, *supra* note 28.
154. *Id*.
155. *Id*.
156. *Id*.
157. See *Busting Myths About the FAA and Unmanned Aircraft, supra* note 22.
158. *Id.*

issues.[159] The objectives of the Agreement on Rulemaking Cooperation Guidelines for the Federal Aviation Administration and the European Aviation Safety Agency are to:

> 1. Exchange rulemaking intentions and priorities of the Participants to align as much as possible their respective rulemaking programmes;
> 2. Identify rulemaking initiatives of common interest that through regulatory collaboration would allow the FAA and the EASA to[160]: (i) avoid unnecessary divergence and duplication of work, (ii) maximize available resources, and (iii) further harmonization.
> 3. Define the corresponding working methods … to be followed by the Participants when executing tasks which have been identified as of 'common interest.[161]

Through collaboration with other countries, such as the European Union, there can be more thorough development of drone laws and solutions to privacy and cybersecurity problems with drone activities.

It is also important to look to global differentiations in the drone laws because countries with laws that give more structure and better provide for businesses within the drone industry will likely gain economic advantages. Companies using drones are likely to move some of their operations to those countries. For example, Jeff Bezos, the founder of Amazon, announced in 2013 that he wanted to use drones to deliver Amazon packages sometime in the future.[162] At that time, the United States had not enacted any laws that prohibited drone operations, however, once Part 107 was enacted, it highly burdened the idea of drone delivery services.[163] Due to the barriers on drone delivery services in the United States, Amazon has begun testing these services in Canada and Australia instead.[164] According to Michael Drobac, senior policy advisor at Akin Gump Strauss Hauer & Feld, "the U.S. has fallen

---

159. *See* Jonathan B. Rupprecht, *The Federal Aviation Administration Rulemaking Process*, *in* UNMANNED AIRCRAFT IN THE NAT'L AIRSPACE 43, 67 (Donna A. Dulo, ed., 2015). According to the United States Code, "[t]he [FAA] shall promote and achieve global improvements in the safety, efficiency, and environmental effect on air travel by exercising leadership with the [FAA]'s foreign counterparts, in the International Civil Aviation Organization and its subsidiary organizations, and other international organizations and fora, and with the private sector." 49 U.S.C. §40104(b) (1994).

160. *Rulemaking Cooperation Guidelines for the Federal Aviation Administration and the European Aviation Safety Agency,* FAA (June 13, 2013), https://www.faa.gov/regulations_policies/rulemaking/media/FAAandEASA.pdf [https://perma.cc/R7VQ-SY32].

161. *Id.*; *see also* Rupprecht, *supra* note 151, at 67–68.

162. *See* Seung Lee, *Amazon's Dream of Drone Package Delivery Can Be Real In 'Less Than Five Years'*, NEWSWEEK (June 29, 2016, 9:49 AM EST), http://www.newsweek.com/amazons-dream-drone-package-delivery-can-be-real-less-five-years-475667 [https://perma.cc/XGG6-XT77].

163. *Id*.

164. *Id*.

behind other developed countries in accommodating drone technology due to FAA's reticence to take action."[165]

Although the United States has not been conducive in the past for drone delivery services, Part 107 could lead the way to better regulatory relations between the government and drone entities within the private sector.[166] One view is that the Part 107's legal framework sets a path where the FAA, with the input of drone delivery companies, can enact laws that accommodate this type of operation and keep more of the drone market within the United States.[167]

Bezos provided another view that, rather than having the FAA focus on drone delivery regulations, it would be faster and provide a more proactive approach if, instead, Congress took on this role and enacted drone delivery service legislation.[168] Finally, there is still a chance that drone delivery services will be permitted on a case-by-case basis under Part 107, but only time will tell if the FAA will allow these types of exceptions.[169] Privacy issues with drone cybersecurity , probably more so with drone delivery services, remain, such as drones getting hacked and packages or personal information being stolen. Whatever the way that drone delivery services are established, it is critical that they encompass solutions to privacy and cybersecurity issues.

Even though United States legislators have currently chosen to avoid enacting privacy and cybersecurity regulations, either because legislators are not tasked with it or it is unclear who is in the best position to handle these issues, other countries have taken measures to try and solve these issues.[170] Legislators have struggled to keep up with the continually advancing drone technologies.[171]

A. Additional Country Specific Solutions

Each country has its own way of handling the regulation of drone technologies, including not addressing it at all. It is important to look at the different solutions around the world to drone privacy and cybersecurity that other countries have implemented in order for the United States to be able to develop the best and most efficient solutions. Appendix A includes a chart of additional countries that have enacted privacy laws that drone operators must

165. *Id*.
166. *Id*.
167. *Id*.
168. *Id*.
169. *Id*.
170. *See* THE LAW LIBRARY OF CONGRESS, REGULATION OF DRONES 11 (2016), https://www.loc.gov/law/help/regulation-of-drones/regulation-of-drones.pdf.
171. *See* Kris Graham, *Kris Graham: FAA Requiring Drone Registration*, CLARION LEDGER (Dec. 16, 2015, 4:07 PM), http://www.clarionledger.com/story/business/businessledger/2015/12/16/kris-graham-faa-requiring-drone-registration/77386932/ [https://perma.cc/4HAV-38RF].

follow, but that are not discussed in depth below.[172] A common theme portrayed in Appendix A is that most of the countries listed have generic laws that require the operator to respect the privacy of persons not involved in the drone operations, but do not specify the requirements the operator must follow regarding another's privacy.[173] The lack of clarity provided by nearly all of these laws perfectly portrays the great size of the issue: how should a drone operator not infringe on other's privacy rights and abide by privacy laws?[174]

1. Australia

The Civil Aviation Safety Authority ("CASA") of Australia claims that "Australia was the first country in the world to regulate remotely piloted aircraft[s], with the first operational regulation for unmanned aircraft in 2002."[175] CASA enacted regulations regarding commercial drone operations on September 29, 2016.[176] Not more than two weeks after these new laws were implemented, the Australian government began a large-scale review of safety under these regulations.[177] The new regulations followed a risk-based model, where drone operations that were seen as less risky fell under more lenient regulations.[178] This type of law has struck a debate between traditional aircraft pilots and the drone industry.[179] Manned aircraft pilots and others involved in air traffic management argue that the regulations are too flexible and allow for unsafe operations.[180] Others in the drone industry disagree and claim that CASA's new regulations allow drone industry competition to increase and be less burdensome on regulatory authorities.[181]

There have been few, if any, cases in Australia where a person succeeded in bringing a violation of privacy claim against a drone pilot for his UAS operations.[182] According to Australian attorney, Matthew Craven, "[u]nless the drone pilot is working for an organization with at least $3 million in annual revenue, 'it is not possible for a private individual to take action against an individual drone pilot under the Privacy Act as it currently

172. *See Drone Laws By Country*, UAV SYS. INT'L, https://uavsystemsinternational.com/drone-laws-by-country/ [https://perma.cc/7NC9-S7UF] (last visited Jan. 2, 2017).

173. *Id*.

174. *Id*.

175. *See* Meenal Dhande, *The Current Scenario of Global Drone Regulations and Laws*, GEOSPATIAL MEDIA & COMMN'S. (Nov. 19, 2016) [hereinafter *Regulation of Drones*], https://www.geospatialworld.net/article/present-global-drone-regulations-laws/ [https://perma.cc/T2B3-FCTA].

176. *Id.*

177. *Id*.

178. *Id*.

179. *Id*.

180. *Id*.

181. *Id*.

182. *See generally* Andy Kollmorgen, *Drones and Australian Law*, CHOICE (Oct. 10, 2016), https://www.choice.com.au/electronics-and-technology/gadgets/tech-gadgets/articles/drones-and-privacy-rights [https://perma.cc/9SSF-UE5V].

stands.'"[183] There are other ways that private individuals can seek a remedy to privacy violations, such as trespass tort law, but the strength of this type of a case remains uncertain.[184]

CASA is similar to the FAA in that it is not tasked with providing solutions to privacy issues brought about by drone activities.[185] CASA acknowledges that drone operations can create privacy concerns, but states, "CASA's role is restricted to aviation safety – privacy is not in our remit."[186] The Office of the Australian Information Commissioner is tasked with handling privacy issues, however, it has not yet issued solutions to privacy questions regarding UAS operations.[187] Further, in 2014, an Australian parliamentary committee advised that current laws should be reviewed to consider if new legislation was needed to solve drone operations impact on privacy rights, however, no changes to the existing laws were ever made.[188] The current laws also do not provide any solutions to cybersecurity threats on drone activities.

2. Canada

In December 2016, Canada initiated a new drone reporting tool for citizens to report drone operations that it believes are unsafe or reckless.[189] This new tool provides people access via their mobile devices to alert the Canadian government of unsafe drone operations and provides specifics of the drone immediately, rather than hoping the individual can remember details later.[190] This mobile reporting tool does not replace the current reporting mechanisms, such as the Civil Aviation Daily Occurrence Reporting System ("CADORS") or reporting to local police any emergencies,[191] that may occur from drone usage.[192] Besides the basic time, date, and location of the reckless drone operation, the incident-reporting mechanism also asks:

- Was the drone flying near an aircraft?

183. *Id*.

184. *Id*.

185. *See Flying Drones/Remotely Piloted Aircraft in Australia*, AUSTL. GOV'T CIV. AVIATION SAFETY AUTH., https://www.casa.gov.au/aircraft/landing-page/flying-drones-australia [https://perma.cc/Y9Z9-7XDZ] (last visited Jan. 3, 2017).

186. *Id*.

187. *See Id*.

188. *See* Regulation of Drones, *supra* note 170.

189. *See* Kirsten Thompson, *Transport Canada Launches Online "Drone Incident" Reporting Tool*, MCCARTHY TÉTRAULT LLP (Dec. 23, 2016), http://www.canadiancybersecuritylaw.com/2016/12/transport-canada-launches-online-drone-incident-reporting-tool/ [https://perma.cc/3TG3-R4FC].

190. *Id.*

191. Transport Canada tells citizens that if they see someone operating a drone "in a way that poses a threat to safety, security, or privacy" that they should contact their local police right away. *See Report a Drone Incident*, TRANSPORT CAN., https://www.tc.gc.ca/eng/civilaviation/opssvs/report-drone-incident.html [https://perma.cc/UWR5-DMHE] (last visited Dec. 29, 2016).

192. *See* Thompson, *supra* note 189; *Report a Drone Incident*, *supra* note 191.

- Was the drone flying at a high altitude?
- Was the drone flying close to an airport/aerodome . . . ? and
- Did the drone fly close to or over . . . a populated area[;] home/private property[;]crowd (sporting event, concert, festival)[;] firework show[;] forest fire[;] national park[;] wildlift[;] moving vehicles, highways, busy streets, bridges
- Give a brief description of the incident[;]
- Description of drone
- Colour, Category,[193] Make/Model
- Description of the operator
- Name of operator and/or company . . .; Operator's vehicle/License plate number . . .[;] physical description . . .
- Have you gathered evidence such as photos or videos of this incident?
- Can a Transport Canada official contact you for more information regarding this evidence?[194]

Further, the form allows the reporter to remain anonymous if he or she chooses.[195] Through this simpler method of incident reporting, it is likely that Canada will have much more information to identify and prosecute illegal drone operations. This reporting method is a wonderful solution to help the government learn about and solve privacy violations by drone operators. For example, if someone is sunbathing in their fenced-in backyard and they notice a drone taking pictures of them, they can immediately report it.

In addition to the new incident reporting tool, the Canadian government has focused on three other key areas.[196] First, Canada announced in the Fall of 2017 the proposed laws for "small drones (25 kilograms or less) that are operated within visual line-of-sight".[197] Previously, this type of drone usage was not covered by legislation, but the government believes these new proposed regulations are necessary in order to clarify how persons can legally conduct this type of drone operations.[198]

Second, the Canadian government has established partnerships with numerous drone manufacturers to better promote safe drone operation.[199] These partnerships require that the participating UAS manufacturers include government safety cards with each drone purchase and participating UAS

193. The form provides pictures of common drones, but also allows for a user to mark that it is unsure of the type of drone. *See infra* App. B.

194. *See Report a Drone Incident*, *supra* note 191.

195. *Id*.

196. *See* Thompson, *supra* note 189.

197. *Id*.

198. *Id*.

199. *Id*.

retailers to include a link to Transport Canada's drone safety website on the retailer's own website.[200]

Third, the Canadian government implemented a "No Drone Zone" campaign to inform the public about drone safety regulations.[201] This campaign focused especially on working with airports to ensure that "No Drone Zone" signs were placed throughout various airport properties, with the hope of minimizing the chance a UAS would interfere with airport or manned aircraft operations.[202]

3. China

In December 2015, the Civil Aviation Authority of China ("CAAC") issued new drone-specific regulations that were to be used on a trial basis before CAAC would decide whether or not to permanently implement them.[203] Soon after these regulations were announced, a drone crashed into power lines in Sichuan, which caused a major blackout and initiated a heated debate regarding drone regulations.[204]

The drone industry is quickly growing.[205] It is especially important that CAAC keep China's laws up-to-date with the industry because . . . .[206] China's regulations cover what lawful drone operations entail, but still focus on the allowance of approved UAS operations to be seen as normal everyday practices. Under the regulations, drones are classified into seven different categories depending on how much they weigh or its specific activities.[207] The strictness of the laws for operation depends on the location of the drone activities, for example, rural locations have more lenient laws while highly populated areas have extremely strict laws.[208] Drones that fall into the first classification are the smallest and have very few regulations to follow, besides not injuring others and conducting safe flights.[209]

Two of the unique and most important regulations established by CAAC are the "UAS Cloud" and the "electronic fence."[210] The "UAS Cloud" is defined as "a dynamic database management system that monitors flight data, including operation information, location, altitude, and speed, in real

200. *Id*.
201. *Id*.
202. *Id*.
203. *See* Dhande, *supra* note 175.
204. *See China: New Drone Regulatory System to Limit Accidents*, https://www.suasnews.com/2016/01/new-drone-regulatory-system-to-limit-accidents/ [https://perma.cc/L88D-Z6JW].
205. *See* Dhande, *supra* note 175.
206. *Id*.
207. *See* App. C; E. Tazewell Ellet et al., *China Launches First Operational Rules for Unmanned Aircraft*, HOGAN LOVELLS (Jan. 20, 2016), http://ehoganlovells.com/rv/ff0024ec11e538d3067f1ce89a4d910aeea3f45d [https://perma.cc/WZ9S-VGLC]; *see also* Dhande, *supra* note 175.
208. *See* Ellet et al., *supra* note 207; *see also* Dhande, *supra* note 175.
209. *See* Ellet et al., *supra* note 207.
210. *See Regulation of Drones*, *supra* note 170, at 39.

time… [and includes] an alarm function for UAS connected to it that is activated when these UAS fly into the electronic fence."[211] The "electronic fence" is defined as "a system consisting of hardware and software that stops aircraft from entering certain areas."[212] Drones that fall into classifications III, IV, VI, and VII are required to use both of these technologies, while also reporting every single second they are operating in highly populated locations and every thirty seconds in less populated areas.[213] UAS that fall into classifications II and V are only required to use the electronic fence and the UAS Cloud, while reporting once a minute if they are flying in specific locations,[214] and airport clear zones.[215]

If the drone operations do not fall under these classifications, they are not required to use the electronic fence or the UAS cloud, but still must include the operators contact information on the drone to allow for easy identification.[216] One way that CAAC could solve privacy issues is to use the electronic fence to block drone operations from going outside specific non-public areas, however, this use is likely to be found to be way too narrow and would not allow for beneficial advancements in the drone industry. CAAC should consider better solutions while still using these technologies to address privacy and cybersecurity concerns. Both the UAS cloud and the electronic fence portray China's ability and desire to use technology to enforce and combat issues arising from new technologies, such as UAS.[217]

Chinese experts have called on CAAC to implement laws that protect a person's privacy from drone operations.[218] These experts have also suggested that more security precautions, such as criminal background checks before one is allowed to operate a UAS, be taken to help address threats to privacy and cybersecurity[219] This is a great model for every country to follow and would help prevent bad actors from joining the UAS community, thereby preventing the occurrence of some malicious and unlawful drone activities.

---

211. *Id*. at 36.
212. *Id*.
213. *Id*. at 39.
214. Specific locations are defined by CAAC as "key areas" that include "military sites, nuclear plants, administrative centers and their neighboring areas, and areas temporarily designated as key areas by local governments." *Id*.
215. *See* Ellet et al., *supra* note 207.
216. *Id*.
217. *See* Dhande, *supra* note 175.
218. *See Absence of Regulations Leaves China's Drone Sector Vulnerable to Security Threats*, BEIJING INT'L, http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1404043.htm [https://perma.cc/4Q8J-D5XY] (last visited Jan. 3, 2017).
219. *Id*.

4. European Union

The European Union's ("EU's") parliament defines a drone as "an aircraft that operates without a crew aboard."[220] Currently, the EU allows for drone operations that are remotely controlled, but not for drone operations that are fully automatic.[221] Most EU countries that have regulated drone operations require that drones weighing more than the 44 – 55 pound threshold (depending on the country) have special authorization before they are flown.[222] Thus far, drones weighing less than 55 pounds have been the most popular in the European region.[223]

The EU is also concerned with increasing the public's knowledge about drone regulations and has created an interactive website as a part of its public awareness campaign.[224] The website informs visitors of both privacy and safety rules by which drone operators must abide.[225] Drone intrusions on privacy and personal data are considered violations of fundamental human rights within the EU.[226] The legislation on this point is general in nature and not drone specific, however, drone operations fall under it.[227] Drone operators should remember that drone operations can easily violate these fundamental rights and that drones that include any type of recording devices must conduct lawful activities under data protection regulations.[228]

One example given by the public awareness campaign is that "you should not take photographs, videos or sound records of people in their home, their garden, their car, etc. without their permission; and remember that data protection and privacy apply even in public spaces."[229] Drones without recording devices can still violate privacy laws.[230] In certain circumstances, privacy laws can also be found to protect personal property.[231] A person who believes their privacy rights have been violated by drone operations may bring a claim against the drone operator either in court or to the national data protection authority.[232]

---

220. *See Civilian Drones: Different countries, different rules*, EUROPEAN PARLIAMENT, http://www.europarl.europa.eu/resources/library/images/20161111PHT50912/20161111PHT50912_original.jpg [https://perma.cc/X7TZ-YRZP] (last visited Jan. 2, 2017).

221. *Id*.

222. *Id*.

223. *Id*.

224. *See Drone Rules*, EUROPEAN UNION, http://dronerules.eu/en/ [https://perma.cc/HR7V-2TJS] (last visited Jan. 2, 2017).

225. *Id*.

226. *See Summary of Privacy Rules in EU*, EUROPEAN UNION, http://dronerules.eu/en/recreational/obligations/summary-of-privacy-rules-in-eu-1 [https://perma.cc/4CRA-PBS9] (last visited Oct. 5, 2017).

227. *See Drone Rules, supra* note 224.

228. *Id*.

229. *See Summary of Privacy Rules in EU*, *supra* note 226.

230. *Id*.

231. *Id*.

232. *Id*.

In July 2016, the European Commission began a partnership between both the public and private sectors to focus on solving cybersecurity threats.[233] By 2020, it is expected that, through the donations from both sectors, 1.8 billion euros will be invested in European cybersecurity initiatives.[234] According to the Commissioner for the Digital Economy and Society, Gunther H. Oettinger:

> There is a major opportunity for our cybersecurity industry to compete in a fast-growing global market. We call on Member States and all cybersecurity bodies to strengthen cooperation and pool their knowledge, information and expertise to increase Europe's cyber resilience. The milestone partnership on cybersecurity signed today with the industry is a major step."[235]

Commissioner Oettinger has exactly the right idea. Collaboration of representatives from all different sectors and entities is the best path for finding a solution that works and solves issues for the industry as a whole. Although the partnership is focused generally on cybersecurity,[236] solutions that come out of it will hopefully be applicable to the drone industry. Further, this partnership is a perfect model for the global drone industry and nation-specific drone industries to follow as to how to create the best solutions for both cybersecurity and privacy issues pertaining to UAS activities.

European organizations are also involved in helping to develop solutions in regard to drone laws. The Innovation and Digital Technologies Division of the European Commission has separated drone operations into three basic categories: open operations, specific operations, and certificated operations.[237] Appendix D displays a chart with more detail regarding the categories, however, while the basic classification of drone operations is useful at clarifying some drone operations, it does not have a good structure for providing which detailed rules operators in each category will have to follow.[238] It also does not explain whether each category will get its own rules regarding each issue or if rules will overlap between the categories.[239]

The Single European Sky Air Traffic Management ("ATM") Research initiative ("SESAR") is an EU entity that develops insights into how its

233. *See Commission Signs Agreement with Industry on Cybersecurity and Steps Up Efforts to Tack Cyber-threats*, EUROPEAN COMMISSION (July 5, 2016), http://europa.eu/rapid/press-release_IP-16-2321_en.htm [https://perma.cc/Q2KB-MUM6].

234. *Id*.

235. *Id*.

236. *Id*.

237. *See Setting Up Rules for Safe Drone Operations in the EU*, EUROPEAN COMMISSION (Nov. 2016), http://ec.europa.eu/transport/modes/air/aviation-strategy/innovation_en [https://perma.cc/2VYF-BHRJ].

238. *Id*.

239. *Id*.

members believe drones should be handled.[240] SESAR proposes that their seven pillars of research, one of which is "security and cyber resilience," are key to enacting proper drone procedures for the EU.[241] SESAR claims that the EU's ability to address cybersecurity threats from drones will be the determining factor in how quickly the entire European UAS industry will grow.[242] Further, SESAR argues that the EU community will become more accepting of drones the longer the period in which no cybersecurity drone incidents occur.[243] Although this is true, drone technologies have already quickly started to play a large role in EU's society.[244]

According to SESAR, one of the best ways for the EU to regulate the UAS industry is to ensure that "the capabilities of drone flights must be preserved for beneficial purposes, meaning risks associated to privacy violations, flights in protected environments, and cybersecurity aspects must be properly managed to avoid negative impacts to society."[245] It is wonderful that SESAR mentions the importance of privacy and cybersecurity regulations and, if followed by the European Commission, it will be a good example for other nations. They will see that it is critical to prioritize these issues. SESAR does address the fact that they have not yet developed clear guidelines on how to solve the cybersecurity issues, but, with proper legislation, it will motivate private entities to help create concrete solutions.[246]

Another argument SESAR makes is that "[p]rivate initiatives are exploring potential solutions such as digital identification but clear concepts of operations, requirements and standards are needed to drive research into a more advanced and coordinated phase."[247] SESAR may not have developed the best solutions to privacy and cybersecurity issues, but simply by working to solve these issues proactively, the EU is likely to be on track to having some of most encompassing regulations.

5. France

France has a very advanced drone industry and was one of the first nations to enact legislation on commercial drone operations.[248] The regulation

240. *See* SESAR JOINT UNDERTAKING, EUROPEAN DRONES OUTLOOK STUDY 2 (Nov. 2016), http://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf [https://perma.cc/7YHS-ZWJK].

241. *Id.* at 6.

242. *Id.* at 10.

243. *Id.* at 16.

244. *See Drones: New EU Rules to Ensure Safety and Privacy*, EUROPEAN PARLIAMENT NEWS (November 11, 2016), http://www.europarl.europa.eu/news/en/news-room/20161107STO50307/drones-new-eu-rules-to-ensure-safety-and-privacy [https://perma.cc/X5BF-4E3J].

245. *See European Drones Outlook Study*, *supra* note 240, at 35.

246. *Id.*at 39.

247. *Id*.

248. *See* Rude Ruitenberg, *What the French Know About Drones That Americans Don't*, BLOOMBERG (Mar. 16, 2015, 6:00 AM), https://www.bloomberg.com/news/articles/2015-03-16/what-the-french-know-about-drones-that-americans-don-t [https://perma.cc/5Q8X-622Z].

of commercial drone operations in 2012 has allowed for the commercial drone industry to grow significantly.[249] According to Redbird's CEO, Emmanuel de Maistre,[250] "France has about a year of advance on the U.S. . . . [t]he regulation created the market."[251] On January 1, 2016, France enacted two regulations regarding civilian drone operations, one of which categorizes drones based on the type of operation.[252] The three categories are "(1) hobby and competition flying, (2) flying for experimental and testing purposes, and (3) 'particular activities', which are defined as any use that does not fall into categories (1) or (2)."[253] While not completely clear, it seems as though commercial operations falls into category 3.[254]

France heavily regulates the areas where drones may fly and these laws are likely to get stricter soon.[255] French legislators are developing a law that would penalize drone operations in prohibited locations.[256] These penalties could include a six month jail sentence and a fine up to approximately $17,500.[257] Another law currently being drafted would require drones weighing over 28 ounces to have extra security devices installed on them.[258] The security devices would prevent drones from entering prohibited areas and alarms would be triggered if the drones lose control.[259] These penalties and additional security devices help to prevent drones from operating outside of the permitted zones,[260] but, in order for the law to be adequate, it should include a clause about how these regulations help protect privacy. The drone regulations in France fail to adequately address privacy and cybersecurity issues, therefore, in these terms, France is not as advanced in the drone sphere as one may think.

6. Germany

One way Germany has addressed privacy and cybersecurity concerns is by enacting laws specifically created to address privacy and protection measures for data obtained through drone operations.[261] Drones that weigh between approximately 11 and 55 pounds must obtain a specific authorization

249. *Id*.

250. Redbird is a French company that uses drones to map construction and mining sites. *See Better Data, Better Decisions,* REDBIRD, http://www.getredbird.com/en/ [https://perma.cc/HC9X-Z6SE] (last visited Jan. 5, 2017).

251. *See Ruitenberg*, *supra* note 248.

252. *See Regulation of Drones*, *supra* note 170, at 43.

253. *Id*.

254. *Id*.

255. See France Gives Lift Off to Tough New Drone Laws, LOCAL (Sept. 28, 2016), http://www.thelocal.fr/20160928/france-draws-up-new-tougher-drone-laws [https://perma.cc/S7A5-9FSQ].

256. *Id*.

257. *Id*.

258. *Id*.

259. *Id*.

260. *Id*.

261. *See Regulation of Drones*, *supra* note 170, at 11.

from the aviation authority before they are allowed to fly.[262] In order to get a specific authorization, one requirement is that the operator submit a data privacy statement.[263] Germany requires these types of specifications be followed; noncomplying drone activity will not be permitted.[264]

The data privacy statement clarifies that data protection and privacy laws are not violated by drone operations. If the drone operations include processing personal data for any other use than "personal or family activities,"[265] the Federal Data Protection Act applies.[266] Drones equipped with a video camera for non-recreational operations also fall under the Federal Data Protection Act.[267] According to the Federal Data Protection Act, "video surveillance of public places may only be conducted to fulfill public tasks, to exercise the right to determine who shall be allowed or denied access to a property, or to pursue rightful interests for precisely defined purposes – for example, protection against theft or vandalism."[268] Drone operations of this nature, even in private areas, still must lawfully process data and have the permission of any persons whose data is taken.[269]

Drones that are not equipped with a camera, but that have one installed and use it to take videos and pictures must abide by the Copyright Arts Domain Act.[270] According to section 22 of this Act, "images can only be disseminated with the express consent of the person concerned."[271] There are exceptions to this regulation. For instance, a picture of society in a contemporary sense that does not conflict with legitimate privacy concerns may be lawful.[272]

People in Germany also have a "General Right of Personality."[273] Both data protection rights and the "Right to Control the Use of One's Image" are included in the General Right of Personality.[274] Not only are people protected from drone operation violations, but also the privacy of their property may be found to be protected.[275] Under Section 2 of Germany's Copyright Act, it can be found that "utilizing a drone to take pictures of public buildings, bridges, sights, or statutes is therefore only permissible if the image is made for private use," however, the outside of buildings in public areas is usually lawful.[276]

---

262. *Id.* at 54.
263. *Id*. at 55.
264. *Id.* at 52.
265. The Federal Data Protection Act defines "personal data" as "any information concerning the personal or material circumstances of an identified or identifiable individual." *Id* at 56.
266. *Id.*at 56–57.
267. *Id*. at 57.
268. *Id*.
269. *Id*.
270. *Id*.
271. *Id*. Disseminated means both public and private circulation, even if only to a small amount of people. *Id*.
272. *Id*.
273. *Id*.
274. *Id*. at 57–58.
275. *Id*. at 58.
276. *Id*.

German privacy laws for drone operations are thus far some of the most clear and efficient in the world. Other countries should look to Germany as a model for privacy laws regarding drones.

Germany has not implemented laws to help protect drones from cybersecurity issues, but this is an area where the United States and Germany may be able to work together to develop regulations. On March 22-23, 2016, the fourth round of the U.S. – Germany Cyber Bilateral Meeting occurred and both countries agreed to work together to protect critical infrastructure from cyber attacks.[277] They also agreed to "continue to work closely to enhance cybersecurity of critical infrastructure, improve incident management and coordination, and build cyber capacity of other countries."[278] It is imperative that leaders within this partnership make drone operations one of the focal points of where cybersecurity issues arise. They must also be proactive in implementing regulations that will continue to adequately regulate as drone technologies advance.

7. Israel

The drone market in Israel is known to be very large, but the market consists mostly of the use of drones for military purposes, not civilian uses.[279] Due to the limited civilian drone operations, partially because of the difficult nature of getting such operations approved, there are not many regulations in Israel for non-military drone flights.[280] It is imperative for Israel to put strong drone regulations in place because the Comorant, the first passenger carrying drone, recently completed its first solo flight.[281] The Comorant is being labeled as a flying car and the Israeli technology firm that created it hopes to have it on the market as soon as 2020.[282]

In Israel, privacy issues related to drone operations are especially a problem with the use of drones by police, yet a privacy violation public uproar has not occurred. Companies are marketing what would normally be seen as privacy-violating services to the Israeli government. For example, when a riot erupted in Jerusalem, "Bladeworx fitted drones with thermal cameras and flew them just ahead of the light-rail trains as they passed near trouble spots.

---

277. *See* Aisha Chowdhry, *U.S. and Germany Expand Cyber Cooperation*, FCW (Mar. 28, 2016), https://perma.cc/manage/create?url=https://fcw.com/articles/2016/03/28/us-germany-cyber.aspx [https://perma.cc/5LQV-4VHD].

278. *Id*.

279. *See* Christa Case Bryant, *What Privacy Debate? Police Drone Use in Israel Flies Under the Radar*, CHRISTIAN SCI. MONITOR (Sept. 19, 2014), http://www.csmonitor.com/World/Middle-East/2014/0919/What-privacy-debate-Police-drone-use-in-Israel-flies-under-the-radar.

280. *See* Aurore Geraud, *Drones in Israel: From Military to Civil Use*, L'ATELIER (Sept. 9, 2016), http://www.atelier.net/en/trends/articles/drones-israel-military-civil-use_443364.

281. *See* Stuart Winer, *Flying Ambulance Heading for Take Off: Israeli-made Cormorant Could be Used to Rescue People in Dangerous Situations, or Ferry Troops in Combat*, TIMES ISRAEL (Jan. 4, 2017), http://www.timesofisrael.com/flying-ambulance-drone-heading-for-take-off/ [https://perma.cc/5LQV-4VHD].

282. *Id*.

. .The drones relay[ed] real-time video to the train operators, police, and even City Hall, enable[ed] officials to spot potential attackers and track those who tried to escape."[283] When the police used drones in this incident, no one mentioned the privacy issues that could occur with government use of thermal camera drone flights.[284] Israel is an example of a country that may have different views on privacy than those in the United States and where it may not be necessary, under those views, to regulate privacy issues.

Israel has also failed to regulate cybersecurity issues related to drone flights, but this is likely to change in the near future. In February of 2016, the Israeli Security Agency and Israeli National Police arrested Majed Awida, who had been asked by the Palestinian Islamic Jihad to hack into the drones belonging to Israel's Defense Forces as well as other areas of the Israeli government.[285] This was not the first time one of Israel's Defense Forces' drones was hacked and, if no measures are quickly put in place, it is unlikely to be the last hack.[286] On December 16, 2016, President Obama signed the U.S. – Israel Advanced Research Partnership Act of 2016.[287] This partnership is a way for the U.S. and Israel to work together to solve cybersecurity issues and provides an opportunity to address these concerns as they relate to drone operations.[288] Israel could likely learn about beneficial regulatory models for drones and the United States. could likely learn a great deal about drone technology advancements.[289] According to United States House Representative John Ratcliff, one of the congressmen that introduced the partnership measure:

> Our discussions with Israeli national security and cybersecurity leaders revealed the immense wealth of untapped potential we can leverage together to collectively vamp up our efforts to combat growing cyber threats . . . We are extremely grateful for the opportunity to work more closely with a country that's a proven pioneer in cyber science and a top leader in cyber expertise.[290]

---

283. *See* Bryant, *supra* note 279. Bladeworx is a company based in Israel. *See* BLADEWORX, http://www.bladeworx.co.il/, (last visited Jan. 5, 2017).

284. *Id*.

285. *See* Elad Popovich, *The 'Palestinian Idol' that Hacked Into Israel's Drones*, SMALL WARS J. (Apr. 1, 2016, 2:00 AM), http://smallwarsjournal.com/blog/the-%E2%80%98palestinian-idol%E2%80%99-that-hacked-into-israel%E2%80%99s-drones [https://perma.cc/32BK-4MWP].

286. *Id*.

287. *See US-Israel Cybersecurity Collaboration Legislation Signed Into Law*, JEWISH TELEGRAPHIC AGENCY (Dec. 20, 2016, 12:06 PM), http://www.jta.org/2016/12/20/news-opinion/politics/us-israel-cybersecurity-collaboration-legislation-signed-into-law [https://perma.cc/5EH8-9P7P].

288. *Id*.

289. *Id*.

290. *Id*.

This partnership will hopefully get Israeli officials to focus on establishing cybersecurity drone laws.

8. New Zealand

New Zealand has drone laws that directly address privacy issues.[291] Regulations on drone operations, including provisions on privacy, came into force in New Zealand on August 1, 2015.[292] One of the regulations requires that drone operators gain consent both from private property owners of land over which they are flying and from any person over which they are flying.[293] New Zealand is similar to Germany in that its Privacy Act applies to drone operations that record people.[294] The Privacy Act 1933 regulates how information about individuals is collected, stored, and disbursed.[295] Although the Privacy Act 1933 is applicable to drones, the Office of the Privacy Commission made sure to note that "the Privacy Act is a technology neutral piece of legislation which gives the basic principles by which we can make an assessment on the privacy implications of an emerging technology."[296]

The New Zealand Privacy Commission states that privacy issues surrounding drones are consistent with the privacy issues surrounding cameras, therefore, New Zealand's CCTV[297] guidelines apply to drones and their operations that involve cameras.[298] In order to abide by the Privacy Act, the CCTV guidelines state that the key issues for any camera operator, such as the operator of a drone with a camera, to observe are:

- Being clear about why you are collecting the information;
- Making sure people know you are collecting the information;
- How you intend to use the information;
- Keeping the information safe and making sure only authorized people can see it;

---

291. *See Regulation of Drones*, *supra* note 170, at 71.

292. *See id.* at 71; *New Zealand: - New Drone Rules Protect Home Privacy*, SUAS NEWS (July 14, 2015), https://www.suasnews.com/2015/07/new-zealand-new-drone-rules-protect-home-privacy/.

293. *Id*.

294. *See Regulation of Drones*, *supra* note 170, at 11.

295. *See* Charles Mabbett, *Game of Drones*, PRIVACY COMMISSIONER (Jan. 21, 2015), https://www.privacy.org.nz/blog/drones/.

296. *Id*.

297. "'CCTV' stands for 'closed circuit television.'" "This term is relatively out of date," but when used by New Zealand's Privacy Commissioner it means "camera surveillance systems that capture images of individuals or information relating to individuals." *See* PRIVACY COMMISSIONER, PRIVACY AND CCTV: A GUIDE TO THE PRIVACY ACT FOR BUSINESSES (2009), https://www.privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/Privacy-and-CCTV-A-guide-October-2009.pdf.

298. *See* Mabbett, *supra* note 295.

- Disposing of the information after it has served its purpose; and
- Right of access to the information by the individual or individuals concerned.[299]

At a minimum, these guidelines provide a framework of issues drone operators should keep in mind to lessen the chance of violating any privacy rights.

In addition to the Privacy Act and the CCTV guidelines, other New Zealand regulations may apply to drones that have the capability to film or take photographs.[300] One of these regulations makes it illegal to take "intimate recordings" of people and publish them when permission to do neither action was given.[301] The example given by the Privacy Commissioner for this regulation states, "if you are sunbathing semi-naked in your own back yard surrounded on all sides by a three metre high fence, you would have an expectation that you won't be spied on."[302] Under this example, if a drone operator was to take pictures of a person sunbathing semi-naked, the person could potentially file an invasion of privacy claim against the operator with the New Zealand courts.[303] Another regulation that applies to drone operations with cameras is Summary Offences Act 1981, Section 30, which makes it illegal to look into and record any activity happening inside a person's home.[304] Although New Zealand has only enacted a couple of regulations specifically related to drone privacy issues, the Privacy Commissioner's blog post provides wonderful guidance that solves many of these issues.[305] Other nations should consider publishing clarifying statements if they do not want to enact permanent legislation that advises drone operators as to how they can avoid any privacy issues from their operations.

Currently, New Zealand does not have any regulations that provide UAS cybersecurity solutions. Officials in other areas of New Zealand's government should consider following the Privacy Commissioner's model of providing clarification through blog posts to address the issues of cybersecurity and drones.

9. Sweden

Sweden recently made important advancements in its privacy laws regarding drones. On October 21, 2016, the Swedish Administrative Supreme Court decided the issue of whether drone operations that involve camera use fell under the definition of "camera surveillance" according to Swedish

299. *Id*.
300. *Id*.
301. *Id*.
302. *Id*. *See also* Crimes Act 1961, ss 216G–216J (N.Z.).
303. *See* Mabbett, *supra* note 295.
304. *Id*.
305. *Id*.

law.[306] The court held that this type of drone operation does constitute camera surveillance, thus, an operator must obtain a license before using drone cameras.[307] These licenses are not easily obtained because the drone operator must show that the benefit of the camera drone operations outweighs the public concern of privacy violations.[308] The cost of a license for camera drone operations ranges from $1,270 per year to $38,095 per hour, with the most expensive licenses being for more professional operations.[309] Critics of this court decision argue that it is too restrictive and overbroad as a way to protect privacy rights, which will have a detrimental effect on the Swedish drone industry.[310] UAS Sweden claims that this court decision could cause a potential loss of 5,000 jobs.[311] Sweden perfectly exemplifies the importance of weighing privacy concerns against economic harm, which is something all countries must consider when implementing new drone regulations. It is too soon to know if the Swedish court decision was a poor way to regulate privacy issues due to a harmful economic effect or if it provides a positive solution to preventing drone operations from violating fundamental privacy rights.

Sweden does not yet specifically regulate cybersecurity drone issues. Due to the privacy law determination in Sweden coming from a court opinion, it may take an actual cybersecurity case to get the Swedish government to provide solutions to drone cybersecurity issues. It is important for Sweden to regulate cybersecurity in drone operations as one way of allowing the UAS industry continue to advance.

10. United Kingdom

According to a drone survey conducted by the United Kingdom Civil Aviation Authority, 48 percent of individuals viewed drone operations as being unregulated throughout the country.[312] The government admitted that it does not have very much evidence that drone operators are purposefully violating privacy laws, however, it still believes that privacy is a concern that must be addressed.[313] Currently, there are privacy focused regulations in place

306. *See Regulation of Drones*, *supra* note 170, at 104; Tonya Riley, *Sweden's Ban on Drone Photography Raises Questions of Privacy*, INVERSE (Oct. 23, 2016), https://www.inverse.com/article/26005-honda-creriding-assist-motorcycle.

307. *See Sweden Bans Cameras on Drones*, BBC (Oct. 25, 2016), http://www.bbc.com/news/technology-37761872.

308. *See* Lisa Vaas, *Sweden Bans Cameras on Drones, Deeming It Illegal Surveillance*, SOPHOS LTD. (Oct. 27, 2016), https://nakedsecurity.sophos.com/2016/10/27/sweden-bans-cameras-on-drones-deeming-it-illegal-surveillance/.

309. *See* JP Buntinx, *Sweden Bans Unlicensed Usage of Camera Drones*, MERKLE (Oct. 28, 2016), http://themerkle.com/sweden-bans-unlicensed-usage-of-camera-drones/.

310. *Id*.

311. *See Sweden Bans Cameras on Drones*, *supra* note 307.

312. *See* CIV. AVIATION AUTH., CONSUMER DRONE USERS 7 (2016), http://dronesafe.uk/wp-content/uploads/2016/11/CAA_Consumer_Drone_Users_report.pdf.

313. *See* DEP'T FOR TRANSP., UNLOCKING THE UK'S HIGH TECH ECONOMY: CONSULTATION ON THE SAFE USE OF DRONES IN THE UK 56–58 (Dec. 21, 2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/579562/consultation-on-the-safe-use-of-drones.pdf.

for the operation of drones that weigh less than 150kg.[314] Under these regulations, drone operations that collect personal data have to abide by the Data Protection Act 1988 ("DPA"), unless the operator has gotten an exception or the use falls under a general exemption.[315] If an operator violates the DPA, the Information Commissioner's Office can penalize the operator by requiring the person to stop that type of operation and/or fining the person.[316] It is also important to note that a person harmed because of a drone operator violating the DPA can bring a case against the operator for monetary compensation.[317]

Another privacy regulation for UAS 150kg or under is that "[d]rones should be flown at a height over the property of another person which is 'reasonable' in all circumstances. Failure to do so could amount to trespass if the flight interferes with another person's ordinary use and enjoyment of land and the structures upon it."[318] The repercussion for trespass is that the victim can bring a civil case against the pilot for monetary compensation and can request that an injunction be put in place to make sure a trespass by this operator's drone does not occur in the future.[319] This law does not provide much guidance. Its subjectivity of the meaning of "reasonable" makes it less effective at properly regulating trespass by drone. While the idea behind it is well intentioned, other countries should consider including a more definite height-based description of when trespass could occur if they implement a similar regulation.

In addition to the regulations already in place, the United Kingdom has begun to lay the groundwork for clearer and more drone-specific laws by establishing a consultation that was announced on December 21, 2016 by the Minister for Aviation in the United Kingdom's Department for Transportation, Lord (Tariq) Ahmad of Wimbledon and will last until March 15, 2017.[320] The consultation allows for people and entities to submit ideas and weigh in on proposed legislation on how to regulate drones and how to solve legal issues regarding operations.[321] Both security and privacy are two of the main focuses of the consultation.[322] One privacy issue for which the United Kingdom is using the consultation for help is the use of cameras and recording devices on drones.[323] The United Kingdom Department for Transport is working with two other main offices, the United Kingdom

314. *Id*. at 18.
315. *Id*.
316. *Id*.
317. *Id*. at 57.
318. *Id*. at 58.
319. *Id*.
320. *Id*. at 8.
321. *Id*. at 7–8.
322. *Id*.
323. *See* Victoria Hordern & Paul Maynard, *UK Department for Transport Launches Consultation on Regulations for Civil Drone Usage*, HOGAN LOVELLS: CHRONICLE DATA PROTECTION (Dec. 23, 2017), http://www.hldataprotection.com/2016/12/articles/international-eu-privacy/uk-department-for-transport-launches-consultation-on-regulations-for-civil-drone-usage/ [https://perma.cc/WEB3-SKLY].

Information Commissioner's Office and the Surveillance Camera Commissioner, to develop drone privacy regulations and ways to make the public aware of how their UAS operations can hamper another person's privacy.[324] The consultation notes that it is the belief of the government that most privacy issues happen because the operator is unaware of the regulations they are violating, however, the government does admit that there are still some violations that are done maliciously.[325] This observation portrays the United Kingdom's motive for not only enacting laws, but also undertaking a public awareness campaign, which will hopefully decrease the amount of privacy and security issues from drone use.[326]

One solution the consultation proposes is the collection of drone operators and owners personal information in order to better enforce the laws and identify persons who are conducting illegal drone activities.[327] Also, the Department of Transport is considering if it should be mandatory for all drones to have a tag that could be scanned to help with identification.[328] According to British privacy law attorney, Victoria Hordern, the tag "would allow an individual drone to be pinpointed to a specific location at a particular time. Not only might this assist with enforcement in . . . possible privacy breaches, but data on the use of drones in particular areas could be utilized to improve coverage of drone-based services."[329] The consultation, especially its inclusion of privacy and security issues, is a great model for the United States and other countries to consider adopting. It allows key members from all sectors of the UAS industry to play a role in regulating drone operations for the greater good and, in the process, it allows people to become more informed about critical legislation that must be followed.

In addition to the consultation, the United Kingdom is solving many of the issues surrounding drones through a public awareness model.[330] The "Drone Code," published by the United Kingdom Civil Aviation Authority, uses unique graphics and a mnemonic device to help those involved in drone operations remember key regulations for safe operations.[331] For example, it is easy to remember the helpful mnemonic device, DRONE, which stands for:

- **D**on't fly near airports or airfields;
- **R**emember to stay below 400ft (120m);
- **O**bserve your drone at all times – stay 150ft (50m) away from people and property;

---

324. *Id*.

325. *See Unlocking the UK's High Tech Economy: Consultation on the Safe Use of drones in the UK*, *supra* note 313, at 19.

326. *Id*.

327. *See Unlocking the UK's High Tech Economy: Consultation on the Safe Use of drones in the UK*, *supra* note 313, at 19.

328. *Id*.

329. *Id*.

330. *See* CIV. AVIATION AUTH., THE DRONE CODE, http://dronesafe.uk/wp-content/uploads/2016/11/Dronecode.pdf (last visited Dec. 30, 2016).

331. *Id*.

- **N**ever fly near aircraft;
- **E**njoy responsibly.[332]

An improvement for this mnemonic device would be to add reminders about not interfering with others privacy and taking the proper measures to ensure an operator's UAS is as secure as possible from cyber attacks. The United Kingdom has failed to adequately address cybersecurity issues. The consultation does not specifically mention any ideas on how these issues might be resolved,[333] the United Kingdom has failed to adequately address cybersecurity issues.

VII. SOLUTIONS

The increase in drone activity calls for an increase in both cybersecurity regulations and privacy laws surrounding it.[334] The easiest, but probably the least popular, solution is to completely ban drone usage. The countries that have currently taken the complete ban approach include Bhutan, Brunei, Cuba, Nicaragua, Uzbekistan, Saudi Arabia, Oman, and Bahrain.[335] It is important to note that remote sensing operations, while sometimes heavily regulated and only used for specific purposes, are still allowed in these countries, even though drone operations are not.[336] While it may be easy to

332. *Id*.

333. *See Unlocking the UK's High Tech Economy: Consultation on the Safe Use of drones in the UK*, *supra* note 313.

334. *See* Stepanovich, *supra* note 80, at 109.

335. *See, e.g.*, Courtney Trenwith, *UAE Enters the Drone Age of Technology*, ARABIAN BUS. PUB. LTD. (Sept. 30, 2016, 12:26 AM), http://www.arabianbusiness.com/uae-enters-drone-age-of-technology-647344.html#.V_miitx1ZR1; *Bhutan Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bhutan-drone-laws/; *Brunei Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/brunei-drone-laws/; *Cuba Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/cuba-drone-laws/; *Nicaragua Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/nicaragua-drone-laws/; *Uzbekistan Drone Laws*, UAS SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/uzbekistan-drone-laws/.

336. *See generally, e.g.*, *Bhutan Customs*, VisaHQ, https://bhutan.visahq.com/customs/, (last visited Jan. 2, 2016); THE LEGAL ASPECTS OF REMOTE SENSING 24 (Geospatial Insight Ltd., 2014); P.J. Blount, *Taiwan, Nicaragua Ink Satellite Imaging Pact*, RES. COMMUNIS BLOG (Oct. 6, 2010, 2:15 PM), http://rescommunis.olemiss.edu/2010/10/06/taiwan-nicaragua-ink-satellite-imaging-pact/; ASIAN DISASTER REDUCTION CTR., MINISTRY OF EMERGENCY SITUATION OF REPUBLIC OF UZBEKISTAN, http://www.adrc.asia/acdr/2010kobe/documents/S2-1_04_Uzbekistan.pdf (last visited Jan 2, 2016); Mohammad Rasooldeen, *Kingdom to use 'LIDAR' for Satellite Imagery*, ARAB NEWS (Jan. 18, 2016), http://www.arabnews.com/saudi-arabia/news/866791; *Oman – Sultanate Looks Towards Space Satellite Technology Forum Begins*, MIDDLE EAST NORTH AFRICA FIN. NETWORK (Oct. 10, 2016), http://menafn.com/1095036157/Oman--Sultanate-looks-towards-space-satellite-technology-forum-begins; *Investigating Land Use and Land Cover Change in Bahrain: 1987-2013*, AM. ASSOC. ADVANCEMENT SCI., http://www.aaas.org/page/investigating-land-use-and-land-cover-change-bahrain-1987-2013 (last visited Jan. 2, 2016).

ban UAS operations, it would hamper both technology and business, which would have further negative implications, such as economic loss. Also, if some countries ban drones and others do not, the gap widens between technologically advanced countries and those that are already being left behind.

Another solution is for Congress to make passing adequate drone privacy safeguards a priority.[337] Electronic Privacy Information Center ("EPIC") suggests a three-pronged regulation encompassing:

> - Use Limitations – Prohibitions on general surveillance that limit drone surveillance to specific, enumerated circumstances, such as in the case of criminal surveillance subject to a warrant, a geographically-confined emergency, or for reasonable non-law enforcement use where privacy will not be substantially affected;
> - Data Retention Limitations – Prohibitions on retaining or sharing surveillance data collected by drones, with emphasis on identifiable images of individuals;
> - Transparency – Requiring notice of drone surveillance operations to the extent possible while allowing law enforcement to conduct effect investigations. In addition, requiring notice of all surveillance policies through the Administrative Procedures Act.[338]

These three aspects would be a good start to having sufficient privacy protections from drone usage. The new legislation would also need to allow for private legal action against other private actors that violate privacy rights.[339] Effective privacy laws dealing with drone activities by the government must have a structure for supervising and auditing to ensure that drone usage remains for proper purposes and does not infringe on civil liberties.[340]

In addition to large scale drone regulations, simple changes or advice can also make a big difference in solving both privacy and cybersecurity concerns that drone operations raise. For example, Hong Kong does have drone-specific laws that it has enacted, but it also includes "recommended areas" for drone operations.[341] Even though Hong Kong's government does not require drone operations to be conducted only in the recommended areas, by providing this advice, it helps clarify areas where drone operators are less likely to run into legal issues. A few other countries, such as New Zealand,

337. Stepanovich, *supra* note 80, at 105.
338. *Id*. at 108.
339. *Id*.
340. *See* ETZIONI, *supra* note 124, at 120.
341. *See Hong Kong Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/hong-kong-drone-laws/.

have also provided guidance statements, or even used social media as a way to clarify rules, or answer questions from the public.[342]

It would be wise for other countries to establish many recommended areas to allow for an increase in drone activities. For example, the United States could recommend areas for drone usage in each county, or if a county is highly populated, then the closest other areas that drone operators are advised to fly. These areas should include places where privacy concerns of others would not arise, such as unpopulated areas. The Best Practices provide small scale and short time solutions, but without federal regulations, safety and privacy concerns will continue to exist.[343]

VIII. CONCLUSION

If commercial drone registrations and operations in the U.S. continue to rise, it is imperative that the industry work quickly and collaboratively to develop privacy and cybersecurity standards to keep up with this expanding rate of drone operations. According to AUVSI, within the next ten years, the United States drone industry will likely help develop around 100,000 jobs and put approximately $82 billion into the economy.[344]

Mississippi UAS attorney, Kris Graham, described the likely future of the drone industry best when he said, "[d]rones are on pace to change society as pervasively as mobile phones and the Internet.[345] Inevitably, there will be bumps in the road as this new technology matures. Both existing businesses and new start-ups can avoid disruption (or worse) by starting out on a proper, legal footing."[346] Drone operations are soon to become integral within our society. Without the proper measures in place, the legal issues that come with increased UAS operations will burden the industry and lessen the benefits. Representatives from around the global UAS community need to work together to develop the best ways to handle privacy and cybersecurity issues. This global approach will allow countries to learn from each other and will provide varying ideas on what regulations work (or do not work) at keeping laws up to date with the continually advancing UAS technology. Without adequate drone laws that address both cybersecurity and privacy, drone operations will get more out of hand. The longer there are no regulations of this type, the tougher it will be to enact clear and acceptable laws in the future.

342. *See* Mabbett, *supra* note 295.

343. *See The Disrupter Series: The Fast-Evolving Uses and Economic Impacts of Drones Hearing Before the Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 40–47 (2015) (statement of Margot E. Kaminski, Assistant Professor of Law, Moritz College of Law).

344. *Id*.

345. *See* Kris Graham, *Regulations Surround Drone Use*, CLARION LEDGER (Sept. 9, 2015, 2:00 PM CT), http://www.clarionledger.com/story/money/business/2015/09/09/regulations-surround-drone-use/71918534/.

346. *Id*.

APPENDIX A: ADDITIONAL COUNTRIES THAT HAVE ENACTED PRIVACY LAWS REGARDING DRONE OPERATIONS

COUNTRY	LAW
Afghanistan	• Drone operations must respect the privacy of others.[347] • Media may not use drone cameras that can cause security issues.
Bahamas	• Drone operators may not fly their drones over property belonging to others, unless they have the property owner's consent.[348]
Bangladesh	• Drone operations must respect the privacy of others.[349]
Bermuda	• Drone operators must obtain permission from all property owners of land the operators plan to conduct drone activities over.[350]
Brazil	• Drone operators may not invade others' privacy.[351]
Dominican Republic	• Drone operators must respect other's privacy.[352]
Ecuador	• Drone operators are responsible for knowing privacy laws and must respect the privacy of others when conducting any drone operations.[353]

347. *Afghanistan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/afghanistan-drone-laws/.

348. *Bahamas Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bahamas-drone-laws/.

349. *Bangladesh Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bangladesh-drone-laws/.

350. *Bermuda Drone Laws,* UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/bermuda-drone-laws/.

351. *Brazil Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/brazil-drone-laws/.

352. *Dominican Republic Drone Laws*, UAV SYS. INT'L. (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/dominican-republic-drone-laws/.

353. *Ecuador Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/ecuador-drone-laws/.

Fiji	• Drone operators must respect the privacy of others when flying a UAS.[354]
French Guiana	• Drone operators must respect others' privacy while conducting any drone operations.[355]
Guatemala	• Drone operators must respect the privacy of others during UAS operations.[356]
Guyana	• UAS operators must respect others' privacy while conducting drone activities.[357]
Haiti	• Drone operators have to respect others' privacy during any drone flights.[358]
Hong Kong	• Prior to any drone operations, the UAS pilot must get permission from any landowner whose property the UAS operations will take place on.[359]
India	• Drone operations may be conducted over private property as long as permission of the landowner has been obtained. Drone operations over public property requires the permission of local authorities before any operations may be conducted.[360]

354. *Fiji Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/fiji-drone-laws/.

355. *French Guiana Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/french-guiana-drone-laws/.

356. *Guatemala Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/guatemala-drone-laws/.

357. *Guyana Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/guyana-drone-laws/.

358. *Haiti Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/haiti-drone-laws/.

359. *Hong Kong Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/hong-kong-drone-laws/.

360. *India Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/india-drone-laws/.

Jamaica	• Drone operators may not fly their drones over either public property or private property, unless they have received consent from the landowner.[361]
Japan	• Drone operators cannot fly over property, unless they have the property owner's permission.[362]
Kazakhstan	• Drone operators must respect the privacy of others when conducting any drone flights.[363]
Kyrgyzstan	• The privacy of others must be respected by any drone operators.[364]
Laos	• When conducting drone flights, the operator must respect others' privacy.[365]
Malaysia	• Drones may not be flown near persons who are not involved with the drone operations.[366]
Mongolia	• Drone operators must respect the privacy of others when operating a UAS.[367]
Myanmar	• UAS operators must respect others' privacy during drone operations.[368]

361. *Jamaica Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/jamaica-drone-laws/.

362. *Japan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/japan-drone-laws/.

363. *Kazakhstan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/kazakhstan-drone-laws/.

364. *Kyrgyzstan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/kyrgyzstan-drone-laws/.

365. *Laos Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/laos-drone-laws/.

366. *Malaysia Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/malaysia-drone-laws/.

367. *Mongolia Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/mongolia-drone-laws/.

368. *Myanmar Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/myanmar-drone-laws/.

Nepal	• Drone operators must respect others' privacy when conducting drone flights. It is also important to note that many Nepal locals have reported drone operations near them that they are unhappy about.[369] • Surveillance of persons by drone operations is strictly prohibited, as it is a violation of privacy.[370]
Pakistan	• Drone operators must respect others' privacy during drone flights.[371]
Panama	• When flying drones, operators must respect the privacy of others.[372]
Philippines	• Drone pilots must respect others' privacy during UAS flights.[373] • The Data Privacy Act does not currently address whether or not drones violate it when using recording devices.[374]
Poland	• A drone operation that entails filming, over private property, may be considered a violation of personal rights and the property owner may file a claim against the operator. (Poland law does not have regulations specific to drones, but the general laws of privacy rights may apply to drone operations.)[375]

369. *Nepal Drone Laws,* UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/nepal-drone-laws/.

370. Purushottam Khatri, *Security Agencies, CAAN Concerned Over Rising Drone-Flying Practices*, RISING NEPAL (Sept. 3, 2016), http://therisingnepal.org.np/news/14165.

371. *Pakistan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/pakistan-drone-laws/.

372. *Panama Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/panama-drone-laws/.

373. *Philippines Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/philippines-drone-laws/.

374. *CAP Regulations On Drones*, DISINI L. OFFICE (Mar. 16, 2016), http://www.elegal.ph/cap-regulations-on-drones/.

375. *Drones – Will the Law Allow Them to Crowd the Sky?*, CMS LAW-NOW (Sept. 22, 2015), http://www.cms-lawnow.com/ealerts/2015/09/drones--will-the-law-allow-them-to-crowd-the-sky?cc_lang=en.

Russia	• Persons not involved with drone operations must have their privacy respected by drone operators.[376]
South Korea	• Drones may not fly over people and drone operations must operate as to respect the privacy of others.[377]
Suriname	• Operators must respect others' privacy when flying their drones.[378]
Tajikistan	• Drone pilots must respect others' privacy when conducting UAS operations.[379]
Thailand	• Drones may not fly over people and operators must respect the privacy of others.[380]
Turks and Caicos	• Drones shall not be flown over persons not involved with their operation and the privacy of others not involved in the flight must be respected.[381]
Vietnam	• Drones cannot fly over people not involved with the drone flight and the privacy of others must be respected by drone operators.[382]

376. *Russia Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/russia-drone-laws/.

377. *South Korea Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/south-korea-drone-laws/.

378. *Suriname Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/suriname-drone-laws/.

379. *Tajikistan Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/tajikistan-drone-laws/.

380. *Thailand Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/thailand-drone-laws/.

381. *Turks and Caicos Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/turks-caicos-drone-laws/.

382. *Vietnam Drone Laws*, UAV SYS. INT'L (Feb. 1, 2016), https://uavsystemsinternational.com/drone-laws-by-country/vietnam-drone-laws/.

APPENDIX B: CANADIAN DRONE INCIDENT REPORT FORM DEPICTIONS

The pictures below are those that are included on the Drone Incident Report Form,[383] which citizens can fill out to report unsafe drone operations.[384] These illustrations are a great way of helping people who are not familiar with different kinds of drones better identify the model of the drone they are reporting. The form also allows the reporter to check a "Not Sure" category or fill out an "Other" box if they cannot precisely identify the drone using the below illustrations.[385] If a person has seen a drone violating their privacy, but is unfamiliar with the types of drones, the depictions aid their identification and better ensure accuracy of the reported descriptive information. It is highly probable that this simple mechanism will greatly increase the ability of the government to then identify and prosecute the drone operator, which exemplifies why this model should be used in other countries' reporting methods.

(Labeled "fixed wing drone")[386]

(Labeled "Fixed Wing Drone")[387]

383. *Drone Incident Report Form*, TRANSPORT CAN., https://www.tc.gc.ca/eng/civilaviation/opssvs/drone-incident-report-form.html (last visited Dec. 29, 2016).

384. *Id*.

385. *Id*.

386. *Id*.

387. *Id*.

(Labeled "Quadcopter")[388]

(Labeled "Quadcopter")[389]

388. *Id*.
389. *Id*.

APPENDIX C: CLASSIFICATION OF DRONE OPERATIONS IN CHINA

CATEGORY	DRONE'S EMPTY WEIGHT (kg)	DRONE'S WEIGHT ON TAKE-OFF (kg)
I	Weight must be between 0kg and 1.5kg	Weight must be between 0kg and 1.5kg
II	Weight must be between 1.5kg and 4kg	Weight must be between 1.5kg and 7kg
III	Weight must be between 4kg and 15kg	Weight must be between 7kg and 25kg
IV	Weight must be between 15kg and 116kg	Weight must be between 25kg and 150kg
V	UAS operations specifically for agricultural use in protecting plants	UAS operations specifically for agricultural use in protecting plants
VI	Operation of "unmanned airships"[390]	Operation of "unmanned airships"[391]
VII	Operations of drones in categories I and II, but are conducted beyond the visual line of sight further than 100 meters	Operations of drones in categories I and II, but are conducted beyond the visual line of sight further than 100 meters.

Note: According to attorneys at Hogan Lovells, "if the empty weight and take-off weight of a UAS are respectively within the parameters of different classifications among Type I to Type IV, it shall be classified as the type with the higher requirements."[392]

390. Ellet et al., *supra* note 207.
391. *Id*.
392. *Id*.

APPENDIX D: CLASSIFICATION OF DRONE OPERATIONS IN THE EU

OPERATION CLASSIFICATIONS	Open	Specific	Certificated
RISK ALLOCATION	Low	The risk level varies and is dependent on the type of operation being conducted.	Traditional amount of risk in aviation related activities.
OPERATIONS	These operations include, but are not limited to: • "Flying own drone • Photography and filming • Industrial operations"[393]	These operations include, but are not limited to: • "Mailing • Infrastructure Inspections • Commercial or Industrial Operations"[394]	These operations will likely be similar to those of traditional aviation and will include the transportation of cargo.
EXAMPLE	A farmer flying a drone over his private property and no one else's property.	A drone operator photographing a sporting match.	A store operating a drone to deliver a package that a customer bought online.
SPECIAL REGULATIONS	None listed	Specific regulations will need to be adjusted to fit the particular operation's risk level.	These operations will at least require: • "[a] Remote pilot license • Certification of drones • Operation Manual"[395]
RULE CLASSIFICATION	The rules that apply to this category are considered rules that pertain to product safety.	Traditional aviation rules will be applied to these types of operations.	Traditional aviation rules will be applied to these types of operations.

393. *Setting Up Rules for Safe Drone Operations in the EU*, *supra* note 237.
394. *Id*.
395. *Id*.

ENFORCEMENT AGENCY	Local police will enforce open drone operations.	Aviation Authorities will enforce specific drone operations.	Aviation Authorities will enforce certificated drone operations.