NOTES

BIRD'S-EYE VIEW: A COMPARATIVE EXAMINATION OF DRONE REGULATION THROUGH THE LENS OF PRIVACY PROTECTION

Allison McGregor[*]

TABLE OF CONTENTS

[*]J.D. Candidate, University of Georgia School of Law, 2021. B.B.A. in Economics, University of Georgia, 2018.

I. INTRODUCTION

A drone's technological advances far exceed the laws that govern it, leaving the privacy of citizens uncertain. Within the last five years, the market for drones has skyrocketed worldwide, opening up doors for major companies such as Amazon and DHL, who have been working on a new delivery system that would put the typical car delivery services to shame.[1] Drones also provide aerial imagery services, infrastructure inspection, mapping and surveying of construction sites, and agricultural services for locating and identifying crop diseases.[2] According to Unmanned Aircraft System (UAS) attorney, Kris Graham, "drones are on pace to change society as pervasively as mobile phones and the Internet."[3]

Yet, the drone's technological advancements challenge certain well-established rights that many people in countries like the United States and those in the European Union take for granted, particularly the right to privacy. The level of protection the law affords privacy rights turns on how privacy is defined. For example, in the context of drone regulation, a drone trespassing on one's land and a drone collecting personal information involves two distinct areas of privacy law in the United States.[4]

This Note compares drone regulations in the United States (U.S.) and the European Union (EU), showing that history and the legal definition of privacy in the EU has allowed the EU to directly implement privacy protections into drone regulations. The EU's treatment of privacy has allowed for a more transparent and forward-looking legal structure for commercial drone companies. The United States' tendency to treat privacy law as an intrusion into physical spaces, rather than as an inherent infringement on one's personal information, has hampered the U.S. government's ability to address drone privacy regulation.

This Note will first lay out the basis of privacy law in each region. It will explain the privacy rules and analyze the reasoning behind these rules. Additionally, this Note will describe current drone regulations in each region: the lack of regulations in the U.S. and the rules in the EU, effective January 1, 2021. This

---

[1] *See* Matt Burgess, *DHL's Delivery Drone Can Make Drops Quicker Than a Car*, WIRED (May 10, 2016), https://www.wired.co.uk/article/dhl-drone-delivery-germany; Frederic Lardinois, *A First Look at Amazon's New Delivery Drone*, TECHCRUNCH (Jun. 5, 2019), https://techcrunch.com/2019/06/05/a-first-look-at-amazons-new-delivery-drone/.

[2] *Market for Commercial Drones to Nearly Triple by 2024*, ROBITICS BUS. REV. (Mar. 29, 2019), https://www.roboticsbusinessreview.com/unmanned/market-commercial-drones-triple-size-2024/.

[3] Jennifer Urban, *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*, 70 FED. COMM. L.J. 1, 44 (2018).

[4] The former describes physical trespass covered by tort law, while the latter would come under data privacy that is usually statutorily regulated.

Note will then show why the U.S. is struggling to regulate drones in a holistic way that protects against various privacy issues and why the EU is able to more efficiently transition to effectively protect privacy in this technological age. Finally, this Note provides suggestions to how, given current property laws, the U.S. can attempt to regulate drone usage in a way that not only protects the right to privacy but also promotes commercial development.

II. BACKGROUND LAWS AND REGULATIONS

A. United States Privacy Law

Privacy protection is a highly valued, well-established right in U.S. legal history. The idea of privacy appears in a variety of sources, from the Second Restatement of Torts preventing trespass,[5] to Fourth Amendment protection from government invasion,[6] to the protection of data privacy.[7] "Privacy is protected in the US by means of a patchwork quilt made up of common law, federal legislation, the US Constitution, state law, and certain state constitutions."[8] The varying definitions of privacy and the underlying principles that back these laws create a divergence in how the law can protect privacy rights.

In 1890, Samuel D. Warren and Louis D. Brandeis were the first to convey the idea of privacy in a Law Review article.[9] They described privacy protection more generally, in the sense that privacy laws protected one's "thoughts, sentiments, and emotions."[10] Their idea of protecting privacy involved preventing the media from taking personal information.[11] Warren and Brandeis focused primarily on what is known in the U.S. today as a "right to personality."[12] They believed that the common law already protected privacy in term's of one's home.[13] The two

---

[5] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1979).

[6] *See* U.S. CONST. amend. IV, § I. (stating that people have a right against unreasonable searches and seizures).

[7] *See* Computer Matching and Privacy Protection Act, 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o)-(r), (u) (2014) (requiring federal agencies to follow certain procedures when computer matching to protect individual privacy).

[8] Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OF OTTAWA L. & TECH. J. 357, 360 (2005).

[9] *See* Samuel D. Warren & Louis D. Brandeis*, The Right To Privacy*, 4 HARV. L. REV. 193 (1890) (discussing the privacy tort as an interest in personality).

[10] *Id.* at 199.

[11] *See id.*

[12] *Id.*

[13] *See id* at 193.

essentially summed up privacy as the "right to be let alone."[14] U.S. law appeared to generally accept and appreciate the right to be let alone, but given its incompatibility with the First Amendment right to free speech, U.S. law never officially accepted this idea.[15] Thus, U.S. law refrained from accepting a specific, formal definition of privacy until the 1960s, when William Prosser wrote a Law Review article defining privacy in a way that endorsed America's views on the right to be let alone.[16]

Prosser's definition of privacy divided privacy rights into four distinct categories of torts to encapsulate the *right to be let alone* in a way acceptable under U.S. law.[17] The four torts regarding breach of privacy include: (1) intrusion upon seclusion,[18] (2) public disclosure of embarrassing private facts,[19] (3) false light publicity,[20] and (4) appropriation of name or likeness.[21] Prosser's article placed Warren & Brandeis's idea of privacy into the second tort category, public disclosure of embarrassing or private facts.[22] The first tort category—intrusion upon seclusion—reflects the basis for how Americans think about privacy in other areas of the law.[23] The privacy of one's physical space or things, generally relating back to physical property, still receives the strongest protection in privacy tort claims and privacy claims generally.[24]

The development of case law under each of these four torts has differed dramatically. For example, the right against public disclosure is one of the most highly praised privacy protections in U.S. tort law.[25] Yet, it provides the individual a relatively small about of protection. For example, in public disclosure cases, defendants almost always win because they only have to prove that the information was either already disclosed or that the public disclosure of such

---

[14] *Id.*

[15] *See* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE, 68 (2015); *see also* Tony Wagner, *The Main Differences Between Internet Privacy in the US and the EU*, MARKETPLACE (Apr. 24, 2017) https://www.marketplace.org/2017/04/24/blog-main-differences-between-internet-privacy-us-and-eu/ ("[In the U.S.] [f]ree speech is paramount, and privacy protections are carved out as exceptions.").

[16] *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383 (1960).

[17] *Id.*

[18] *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977).

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] Judith DeCew, *Privacy*, THE STAN. ENCYCLOPEDIA OF PHIL. (Aug. 9, 2013), https://plato.stanford.edu/archives/spr2015/entries/privacy/#Bib.

[23] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161–62 (2004).

[24] *See* Levin & Nicholson, *supra* note 8, at 361.

[25] *See* David A. Anderson, *The Failure of American Privacy Law*, *in* 4 THE CLIFFORD CHANCE LECTURES, PROTECTING PRIVACY, 139, 141 (Basil S. Markesinis ed., Oxford Univ. Press 1999).

information was not highly offensive.[26] While this right against public disclosure has received more focus in recent years, its protection varies from state to state and is highly volatile in who it protects.[27] On the other hand, "intrusion upon seclusion," which encompasses the idea of physical trespass, is highly protected and enforced.[28] The law against trespass gives individuals "an almost absolute right to exclude others from [their] property."[29] From the Restatement (Second) of Torts regarding "intrusion upon seclusion," states have adopted laws mainly aimed at protecting against physical intrusion.[30]

The Court has long defined privacy protections under the Constitution as protecting against intrusion into physical spaces. For example, the Fourth Amendment includes a right to be free from unwarranted government searches and seizures.[31] Historically, the right to privacy under the Fourth Amendment keeps the government off of one's property and out of one's home.[32] Over time, the Court attempted to shift the idea of privacy from protecting one's property to protecting one's reasonable expectation of privacy, but the need for a physical barrier continually limits this transition. For example, in *Katz v. United States* the Court diverged from the idea of physical trespass, stating, "the Fourth Amendment protects people, not places."[33] The plurality concluded that the Fourth Amendment applies whenever a person exhibits an "actual . . . expectation of privacy" that "society is prepared to recognize as 'reasonable.'"[34]

After *Katz*, the Court seemed to move toward protecting privacy in the technological era, yet the idea of spatial privacy came back in full force in *United States v. Jones*.[35] When Jones argued that putting a Global Positioning System (GPS) tracker on his car violated the Fourth Amendment, the Government argued that *Katz* warranted the search because there was no reasonable expectation of privacy on the open road.[36] The Supreme Court, however, disagreed. Applying a historical analysis, the Court considered the GPS installation onto Jones' vehicle as a physical intrusion. Thus, the Court held that the Government conducted an

---

[26] *See id.*

[27] *See Right of Publicity*, FINDLAW, https://corporate.findlaw.com/litigation-disputes/right-of-publicity.html (last updated May 26, 2016) (explaining that "some states only recognize the right of publicity for celebrities while others protect all individuals if the identity is use for commercial advantage").

[28] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1979).

[29] *See* Anderson, *supra* note 25, at 159.

[30] RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1979).

[31] U.S. CONST. amend. IV.

[32] *See* Boyd v. United States, 116 U.S. 616 (1886) (finding that physical trespass onto one's land and going through one's personal property constituted an unwarranted search and seizure).

[33] Katz v. United States, 389 U.S. 347, 351–52 (1967) (plurality opinion).

[34] *Id.* at 361 (Harlan, J., concurring).

[35] United States v. Jones, 565 U.S. 400 (2012).

[36] *Id.* at 406.

unwarranted search under the Fourth Amendment.[37] It follows that while the Court has attempted to enter into the world of viewing privacy protections as one's reasonable "expectation of privacy," the physical invasion rule remains the predominant view on Fourth Amendment privacy protections.[38]

The Supreme Court not only defines the Fourth Amendment protection as a physical one; the Court defines the rights of the Fourteenth Amendment in a similar manner.[39] The Supreme Court focused on spatial boundaries, specifically the marital bedroom, to find that the right to use contraceptives[40] and the right to engage in private sexual activities[41] are fundamental private rights the Government cannot infringe on or deny.

While the rulings in *United States v. Jones* and *Griswold v. Connecticut* do not necessarily affect privacy rules over third-party actors, [42] many forms of U.S. privacy law follow the idea of spatial privacy, including data protection laws. The U.S. protects privacy as a form of physical space rather than a form of identity.[43] In the drone world, the current physical legal protections authorized a man in Kentucky to shoot down a drone flying over his house.[44] So, even though the

---

[37] *Id.* at 407.

[38] *See* Kyllo v. United States*,* 533 U.S. 27, 34–35 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' (citation omitted) constitutes a search—at least where . . . the technology in question is not in general public use."). *But see* United States v. Jones, 565 U.S. 400, 425 (2012) (Alito, J., concurring) ("[T]he Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints."); *see also* Matthew S. Schwartz, *Court Says Using Chalk of Tires for Parking Enforcement Violates Constitution*, NPR (April 23, 2019), https://www.npr.org/2019/04/23/716248823/court-says-using-chalk-on-tires-for-parking-enforcement-violates-constitution (noting that "parking enforcement officers could sidestep the constitutional issue altogether by simply taking a photo of the car rather than using chalk" to physically mark on the cars).

[39] *See Due Process of Law*, JUSTIA, https://law.justia.com/constitution/us/amendment-14/04-due-process-of-law.html#63 (last visited Dec. 26, 2020).

[40] *See* Griswold v. Connecticut, 381 U.S. 479 (1965).

[41] *See* Lawrence v. Texas, 539 U.S. 558 (2003).

[42] United States v. Jones, 565 U.S. 400, 417 (2012). Not only does the Fourth Amendment not protect privacy infringement from third party actors but the third party doctrine, established in *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979), states that if you do give information to a third party then there is no expectation of privacy and that the government has a right to that information.

[43] *See* Whitman, *supra* note 23, at 1210 (distinguishing a "right of publicity" in the U.S. from the right of privacy in the EU by defining a "right of publicity" as "an interest in one's property, not an interest in one's honor.").

[44] Chris Matyszczyk, *Judge Rules Man Had Right to Shoot Down Drone Over His House*, C|NET (Oct. 28, 2015, 11:13 AM), https://www.cnet.com/news/judge-rules-man-had-right-to-shoot-down-drone-over-his-house/.

U.S. protects physical electronic trespass on one's property, the law governing data infringement—or the protection of one's identity—is uncertain. For instance, in a class action suit, a California court denied the class's claim that Facebook violated their privacy rights when Facebook collected URLs of webpages consumer Plaintiffs visited and used persistent cookies to associate their identities with their web browsing histories.[45] The Court concluded the Plaintiffs had no reasonable expectation of privacy since they could have done more to block the cookies, and given the routine use of cookies, these intrusions were not highly offensive.[46] After *In re Facebook Tracking Litigation*, the burden of proving a highly offensive invasion has been higher when the intrusion is of one's personal information rather than one's personal property.[47] Discussed further below,[48] privacy law that focuses on the intrusion into physical spaces underlies many privacy-based regulations, including regulations that affect commercial drone usage.[49]

B. European Union Privacy Law

Privacy in the EU is unified around a single interest: the right to control the sorts of information disclosed about oneself.[50] The basis for this fundamental right is found in Article 8 of the European Convention on Human Rights,[51] as well as the Charter of Fundamental Rights.[52] These treatises provide protection for private and family life as well as personal data.

The protection of privacy in the EU is more focused on protecting one's identity. Similar privacy protections are seen in the wide number of cases addressing a member of royalty against the media.[53] The EU strongly believes in a right to personhood, "founded in the commitment to a society in which every person, of every social station, has the right to put on a respectable public face; a society in

---

[45] *See* In re Facebook Tracking Litig., 263 F. Supp. 3d 836, 846 (N.D. Ca. 2017).

[46] *Id.*

[47] *See Id.*

[48] *See infra* part III.C.

[49] *See* RICHARDS, *supra* note 15 (explaining invasion-based theories of privacy law lie behind laws prohibiting eavesdropping and wiretapping to laws outlawing video voyeurism and harassment by paparazzi).

[50] *See* Whitman, *supra* note 23, at 1161.

[51] See Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, para. 1, Nov. 4, 1950, 213 U.N.T.S. 221, 230.

[52] *See* Charter of Fundamental Rights of the European Union, arts. 7–8, 2000 O.J. (C 364) 1, 10.

[53] *See* Entscheidungen des Bundesgerichtshofes in Zivilsachen [BGHZ] [Supreme Court] Dec. 19, 1995, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 1996, 1128 (Ger.) (Princess Caroline of Monaco); Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Feb. 14, 1973, NJW 1973, 1221 (Ger.) (Princess Soraya of Iran); Von Hannover v. Germany, 40 Eur. H.R. Rep. 1 (2005) (Prince Ernst August of Hanover).

which privacy rights are not just for royalty, but for everybody."[54] The idea of personhood is deeply embedded in these member states' history.

Privacy law that focuses on protecting one's identity developed from the law of insult during the Nazi era and the status revolution in many of the European states.[55] As James Whitman concludes, the "privacy protections offer perhaps the paradigmatic example of high-status norms that have been generalized to the wider population."[56] "When continental lawyers speak of 'privacy' as a set of rights over the control of one's image, name, and reputation, and over the public disclosure of information about oneself, they are speaking to these selfsame continental sensibilities."[57] In choosing strong protections for personal information, the EU is choosing privacy over the right to free speech.[58]

The fundamental idea of privacy law in the EU is entirely distinct from property law protections. The EU does not have one system of property law like they do privacy.[59] Each member state has its own property laws.[60] The separation between privacy and property law has made it much easier for the EU to put any law that deals with one's personal information or identity under Article 8 of the European Convention.[61]

The protection of personal information is also seen in the protections the EU affords personal data. European lawyers believe the trafficking of consumer data is "a serious potential violation of the privacy rights of the consumer if marketers can purchase data about his or her preferences, and regulation is thus imperative."[62]

---

[54] *See* Whitman, *supra* note 23, at 1211.

[55] *Id.* at 1169.

[56] *Id.*

[57] *Id.* at 1167.

[58] *See* RICHARDS, *supra* note 15, at 55.

[59] Christian von Bar, *European Property Law as New Private Law?*, JOTWELL (July 12, 2016), https://property.jotwell.com/european-property-law-as-new-private-law/#targetText=The%20European%20Union%20does%20not,impact%20on%20national%20property%20law.

[60] *See, e.g.*, Cour d'appel [CA] [regional court of appeal] Paris, May 25, 1867, 13 A.P.I.A.L. 247 (Fr.) (concluding that there was a right to one's "image" that was distinct from, and in tension with, rights of property); REGERINGSFORMEN [RF] [CONSTITUTION] 2:8 (Swed.) (giving a person the right to access, walk, cycle, ride, ski, and camp on any land—with the exception of private gardens, the immediate vicinity of a dwelling house and land under cultivation); Land Reform Act 2003, (ASP 2) (Scot.) (establishing statutory public rights of access to land and making provisions under which bodies representing rural and crofting communities may buy land).

[61] *Article 8: Respect for Your Private and Family Life*, EQUITY AND HUM. RTS. COMMISSION, https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life (last updated Nov. 15, 2018).

[62] *See* Whitman, *supra* note 23 at 1192.

The broadest and most protective EU privacy law is the General Data Protection Regulation (GDPR), approved in 2016 and entered into force in 2018.[63] GDPR's strong protections demonstrate how broadly the EU defines personal information and applies it within the law. For example, individuals may be identified by online identifiers available through their devices, like IP addresses and cookie identifiers.[64]

GDPR has strict regulations to ensure that an individual's privacy is protected.[65] For instance, GDPR involves a much higher bar for consent,[66] going from a controller's implied consent to requiring that the controller explicitly consents.[67] GDPR also provides for much stricter regulations concerning when companies must disclose a data breach.[68] Along with more protection and transparency, the regulations also afford individuals more power. GDPR grants a "right to be forgotten," giving an individual the power to demand companies either delete their personal information or not share or sell their personal data.[69] GDPR also contains an accountability principle, requiring the controller to demonstrate compliance with other personal data processing principles.[70] Moreover, GDPR includes fines for those who violate the rules.[71]

---

[63] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]; *see European Union—Data Privacy and Protection*, INTERNATIONAL TRADE ADMINISTRATION, https://eur-lex.europa.eu/eli/reg/2016/679/oj (last visited Dec. 26, 2020) (explaining the breadth of this regulation).

[64] GDPR, *supra* note 63 at ¶ 30.

[65] Ben Wolford, *What is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/#:~:text=The%20General%20Data%20Protection%20Regulation,to%20people%20in%20the%20EU (last visited Nov. 1, 2020).

[66] The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." GDPR, *supra* note 63.

[67] *See* Allison Callahan-Slaughter, *Lipstick on a Pig: The Future of Transnational Data Flow Between the EU and the United States*, 25 TUL. J. INT'L & COMP. L. 239, 251 (2016).

[68] Jay Cline, *Data Breach Notification: 10 Ways GDPR Differs From the US Privacy Model*, PWC (Dec. 2016), https://lists.riskbasedsecurity.com/pipermail/breachexchange/2016-December/000966.html ("[Regulations] that pose a risk of harm to individuals' 'rights and freedoms' must be reported . . . without undue delay and, where feasible, not later than 72 hours after having become aware of it.").

[69] *See* Callahan-Slaughter, *supra* note 67, at 251.

[70] W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. L. 221, 223 (2016–2017).

[71] *Id.* at 229–30.

One of the biggest differences between GDPR and most data privacy law in the U.S. is that the GDPR applies to data held in the private sector.[72] GDPR mandates that businesses adhere to basic privacy principles regarding the way they use individuals' data.[73] The regulations turn more toward protecting the individual rather than the corporation. As James Whitman states: "The basic issue is … not just one of market efficiency. Consumers need more than credit. They need dignity."[74] The idea of privacy as found in Article 8 of the Convention through GDPR remains true in other areas where the EU has implemented privacy protections.[75]

The fundamentals of U.S. and EU privacy regulations are reflected in the current state of their drone regulations.

C. Commercial Drone Regulations in the United States

The Federal Aviation Administration (FAA) is tasked with governing drone usage in the U.S.; however, most drone regulation has fallen in the hands of individual states. In 2012, Congress tasked the FAA with "develop[ing] a comprehensive plan to safely accelerate the integration of civil[76] unmanned aircraft systems [drones] into the national airspace system."[77] The FAA has not implemented any regulations nor answered any questions resolving the concern of drone usage and privacy.[78] Congress has introduced federal regulations, such

---

[72] *See* Solveig Singleton, *Privacy and Human Rights: Comparing the United States to Europe,* COMP. ENTER. INST. (Nov. 30, 1999), https://cei.org/studies-issue-analysis/privacy-and-human-rights-comparing-united-states-europe.

[73] Wagner, *supra* note 15.

[74] *See* Whitman, *supra* note 23, at 1192.

[75] Peter Noorlander, *Privacy in Telecommunications—A European and an American Approach*, E.H.R.L.R. 2, 237 (1999) (explaining that under Artile 8 "the right to respect for private life has been held to extend to issues of one's personal identity, self-fulfillment, sexual activities, family and other relationships and business activities").

[76] *See* Mike Ahlers, *FAA Takes Initial Steps to Introduce Private Drones in U.S. Skies,* CNN (Nov. 7, 2013, 2:08 PM), https://www.cnn.com/2013/11/07/us/faa-drones-over-us/index.html (noting that commercial drone usage has been allowed on a case by case basis but has not been adopted by any actual regulations).

[77] ALISSA M. DOLAN & RICHARD M. THOMPSON II, CONG. RSCH. SERV., R42940, INTEGRATION OF DRONES INTO DOMESTIC AIRSPACE: SELECTED LEGAL ISSUES 2 (2013), https://fas.org/sgp/crs/natsec/R42940.pdf.

[78] *Id.* ("[T]he text of this act . . . fails to address significant, and up to this point, largely unanswered legal questions. For instance, several legal interests are implicated by drone flight over or near private property."). The FAA has implemented new regulations that could also allow UPS to be the first ever drone airline, however, none of these regulations mention anything about privacy. *See* Ken Quinn, Jennifer Trock, & Chris Leuchten, *FAA Unveils New Proposals for Commercial Drone Operations at Night and Over People*, UAS INSIGHTS (Jan. 28, 2019), http://www.uasinsights.com/2019/01/28/faa-unveils-new-proposals-for-commerci

as the Drone Aircraft Privacy and Transparency Act of 2013[79] and the Preserving American Privacy Act of 2013,[80] but neither of these Acts have progressed since 2013.[81] On December 26, 2019, the FAA announced a proposed rule requiring individual drones to include remote identification on their aircrafts.[82] While the implementation of this regulation is a major step in attempting to regulate and allow commercial drone delivery, the FAA will not completely implement the rule for three years.[83] Further, there is no explicit regulation aimed to promote privacy concerns of the customers of a drone delivery company.[84] Thus the FAA has left it up to the courts to regulate and address privacy concerns stemming from drone usage.

Individual states have attempted to regulate drone usage and protect privacy. For instance, in California a person is liable for physical invasion of privacy when they trespass onto one's land to capture any type of image or recording of a person engaging in private activity in a manner that would be offensive to a reasonable person.[85] While the California bill is based on the idea of invasion into a physical space, it does not expand liability "for constructive invasion of privacy for the same activity, as specified, through the use of any device, regardless of whether there is a physical trespass."[86] On the other hand, Wisconsin prohibits drone use when there is a "reasonable expectation of privacy," and Wisconsin courts have found that a reasonable expectation of a privacy can apply in places beyond where a person is actually secluded.[87]

---

al-drone-operations-at-night-and-over-people/; Elizabeth Miller, *Federal Aviation Administration Certifies UPS to Become Fist Ever Drone Airline*, BAKER STERCHI COWAN & RICE BLOG (Nov. 7, 2019), https://www.bscr-law.com/?t=40&an=98715&format=xml&stylesheet=blog&p=5258.

[79] Drone Aircraft Privacy and Transparency Act of 2013, H.R. 1262, 113th Cong. (1st Sess. 2013) (proposing regulations of the private use of drones including data collection requirements and enforcement mechanisms).

[80] Preserving American Privacy Act, H.R. 637, 113th Cong. (1st Sess. 2013) (regulation prohibiting the use of drones to capture images that would be highly offensive to an individual in which he had a reasonable expectation of privacy). This bill could also be read to preempt state regulation of drone flights between states which would impede on commercial drone usage.

[81] *See* DOLAN, *supra* note 77, at 19.

[82] *See* Press Release, Federal Aviation Administration, U.S. Department of Transportation Issues Proposed Rule on Remote ID for Drones (Dec. 26, 2019), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=24534.

[83] Will Feuer, *New Rule Would Make it Possible to Track and Identify Nearly all Drones Flying in the US*, CNBC (Dec. 26, 2019, 1:09 PM), https://www.cnbc.com/2019/12/26/faa-remote-id-rule-for-drones-would-enable-tracking-identification.html.

[84] *Id.*

[85] *See* Cal. Civ. Code § 1708.8. (West 2016).

[86] *See id.*

[87] *See* WIS. STAT. ANN. § 942.10 (West 2014). Note that this right to privacy applies only to a person and may not protect from a drone taking photos of one's property if no person is

Other states have expanded on the idea of a "reasonable expectation of privacy" and given individuals a private right of action to pursue drone violations. For example, Florida passed a law that protects individuals from local drone searches and seizures.[88] That provision defines a reasonable expectation of privacy as one that is "not observable by persons located at ground level in a place where they have a legal right to be, regardless of whether he or she is observable from the air with the use of a drone."[89] While the Florida law only applies to law enforcement agencies, an Oregon drone law creates a private right of action for anybody who "owns or lawfully occupies real property" against any person flying a drone over such property.[90] Although many states in the U.S. are attempting to protect against invasions of privacy stemming from drone usage, the way each state views privacy and regulates privacy varies dramatically.

D. Commercial Drone Regulations in the European Union

The EU has been on the forefront of uniform drone regulations that consider privacy concerns. On June 11, 2019, the EU published the Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems ("EU Drone Regulation").[91] EU Drone Regulation officially went into effect on July 1, 2020, and on January 1, 2021, it officially replaced any national rules of individual member states.[92] Patrick Ky, Executive Director of the European Union Aviation Safety Agency, stated after the initial proposal of the regulation that "Europe will be the first region in the world to have a comprehensive set of rules ensuring safe, secure and sustainable operations of drones both, for commercial and leisure activities. Common rules will help foster investment, innovation and growth in this promising sector."[93]

---

present. *See* Kevin David Trost, *Up, Up and Away: Rising Legal Regulation of Drone Operation*, STATE BAR OF WISCONSIN (Sept. 1, 2016), https://www.wisbar.org/newspublications/insidetrack/pages/article.aspx?Volume=89&Issue=8&ArticleID=25060.

[88] FLA. STAT. § 934.50 (2017).

[89] *Id.*

[90] OR. REV. STAT. § 837.380 (2016).

[91] Commission Delegated Regulation 2019/945 of 12 March 2019, O.J. (L 152/1). *See* EASA, *Civil Drones (Unmanned Aircraft)*, https://www.easa.europa.eu/drones-regulatory-framework-timeline (last visited Nov. 14, 2019) (showing a timeline for implementing the new regulation).

[92] *See* Sarah Moens, *The Future European Drones Regulation: Per Aspera ad Astra,* DLA PIPER (June 14, 2019), https://www.dlapiper.com/fr/france/insights/publications/2019/06/european-drones/.

[93] *EU Wide Rules on Drones Published*, EASA (June 11, 2019), https://www.easa.europa.eu/newsroom-and-events/press-releases/eu-wide-rules-drones-published. During the next High-Level Conference on Drones, taking place in December of 2019, the EASA will discuss the new rules and upcoming regulatory proposal in depth.

Generally, the rules and procedures for drone personnel are based on three categories: open, specific, and certified.[94] A drone in the open category has "a weight limit of 25kg, and a flying distance limit of 120m from the close point of surface, [and] has been determined for a UAS to be able to fly without prior authorization."[95] Commercial drones fall in the certified category because commercial drone operations have a higher risk for third-party injury, which includes drones that operate over assemblies of people, involve the transport of people, or involve the carriage of dangerous goods.[96] Companies that have drones under the certified category must register them and meet certain requirements in their application.[97] Further, "[c]onsidering the risks to privacy and protection of personal data, operators of unmanned aircrafts [drones] should be registered if they operate an unmanned aircraft which is equipped with a sensor able to capture personal data."[98]

The EU Drone Regulation specifically addresses the protection of privacy. The EU Drone Regulation states that "[n]ational registration systems should comply with the applicable Union and national law on privacy and processing of personal data and the information stored in those registration systems should be easily accessible."[99] The EU Drone Regulation directly integrates the EU GDPR. Again, all of these privacy regulations stem from the fundamental right of privacy found in Article 8 of the European Convention of Human Rights and Fundamental Freedoms.[100]

---

[94] *See* EASA, *Drones—Regulatory Framework Background,* https://www.easa.europa.eu/domains/civil-drones-rpas/drones-regulatory-framework-background (last visited Mar. 31, 2021).

[95] *European Commission Rules on the Operation of Drones*, FENCH FARRUGIA FIOTT LEGAL (Sept. 24, 2019*),* https://www.fff-legal.com/european-commission-rules-on-the-operation-of-drones/.

[96] Commission Delegated Regulation 2019/945 of 12 March 2019, art. 5(1), 2019 O.J. (L 152/1).

[97] Commission Implementing Regulation 2019/947 of 24 May 2019, art. 14, 2019 O.J. (L 152/1) 45. Requirements include name and contact information for operators, insurance policy number, and manufacturer designation and serial number.

[98] *Id.* ¶ 16.

[99] *Id.* ¶ 19.

[100] *See* Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, ¶ 1, Nov. 4, 1950, 213 U.N.T.S. 221, 230.

III. ANALYSIS

A. Lack of United States Regulation and Usage

Based on EU's drone regulation, EU commercial drone usage is predicted to grow tremendously in the coming years compared to drone usage in the United States. Data shows that the EU is currently leading in civilian drone use with 2,500 operators, more than the total number of operators in the rest of the world.[101] Research also shows that "the European drone market was valued at €197 million in 2017 and is forecast to reach as much as €3.9 billion by 2039."[102] A primary reason for this increased growth is that "[m]anufacturers and regulators are finally working together to spearhead the effort to integrate unmanned aerial aircraft into their existing air traffic management faster than most other cohesive geographical markets."[103]

The United States, however, lacks a universal commercial drone regulation. While the FAA has taken some initial steps toward regulation, U.S. commercial drone usage is hampered due to Congress's inaction and failure to provide answers.[104]

A proper solution will draw from the strengths of existing U.S. privacy laws and try to unite them into a comprehensive, uniform regulation. The strongest privacy protection in the United States protects against intrusion into physical spaces, while the GDPR affords more protection to personal information.[105] EU's conceptualization of privacy as protecting personal information made it easier to incorporate both physical intrusion and data protection into their drone regulations. Unfortunately, "[r]ather than a single law, a continually broadening assemblage of statutes, regulations, common law duties, contractual commitments, industry norms, and international obligations govern

---

[101] *Regulation of Drones: European Union*, LIBRARY OF CONG., https://www.loc.gov/law/help/regulation-of-drones/european-union.php#_ftnref41 (last updated Aug. 6, 2019).

[102] Juan Plaza, *What is the Value of the European Drone Market?*, COMMERCIAL UAV NEWS (Oct. 15, 2019), https://www.commercialuavnews.com/europe/value-european-drone-market.

[103] *Id.*

[104] Some of these steps include approving drone flights on a case-by-case basis, developing seven drone test sites, and implementing the remote ID system. *See* Ahlers, *supra* note 76; *UAS Test Sites*, FED. AVIATION ADMIN., https://www.faa.gov/uas/programs_partnerships/test_sites/ (last modified May 6, 2020, 2:12 PM); *see also* Feuer, *supra* note 83.

[105] *See* Whitman, *supra* note 23, at 1161.

U.S. data privacy practices."[106] Thus, before suggesting any regulations, this Note will look at other areas of U.S. law that invoke drone privacy issues.

B. Drone Privacy Right Infringement

Commercial drone usage could cause a plethora of privacy infringements. First, trespass, derived from the tort of intrusion upon seclusion,[107] is easily foreseeable and has been regularly litigated in several states.[108] Second, drones provide many other technological advancements that could interfere with one's privacy. Drone surveillance is likely to involve video surveillance, voice recording, location tracking, and facial recognition.[109]

Additionally, drones are equipped with thermal imaging and the capacity to intercept wireless communications, along with other services that can track personal data, including equipment that could scan the products in one's home and target them with advertisements.[110] A number of different laws address these issues,[111] such as state wiretapping laws, peeping tom laws, eavesdropping laws, video voyeurism laws, and data protection laws.[112] All of these laws view and protect privacy in a different way.[113]

C. United States Data Privacy

Before considering drone regulation through data protection laws, there must be an understanding of how U.S. law defines, governs, and protects personal data. The Federal Trade Commission (FTC) is the agency tasked with regulating

---

[106] Samantha Cutler, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1514–15 (2018).

[107] *See* Deteresa v. American Broadcasting Companies, Inc., 121 F.3d 460, 461, 465, *cert. denied* 523 U.S. 1137, 118 S.Ct. 1840, 140 L.Ed.2d 1090 (1998).

[108] *See* Chris Matyszczyk, *supra* note 44; Jason Koebler, *The Sky's Not Your Lawn: Man Wins Lawsuit After Neighbor Shotgunned His Drone*, VICE (June 28, 2015, 8:00 AM), https://www.vice.com/en_us/article/xywjd3/the-skys-not-your-lawn-man-wins-lawsuit-after-neighbor-shotgunned-his-drone.

[109] *See* Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CAL. L. REV. CIR. 57, 59 (2013).

[110] M. Ryan Calo, *The Drone as Privacy Catalyst,* 64 STAN. L. REV. ONLINE 29, 30 (2011).

[111] Because this note is focused on commercial drone usage, it will not discuss privacy laws governing drone usage of government entities such as the Right to Record and other laws regarding Fourth Amendment search and seizure.

[112] Holland Michel & Dan Gettinger, *Drone Incidents: A Survey of Legal Cases*, CTR. FOR THE STUDY OF THE DRONE AT BARD COLL. (Apr. 2017), https://dronecenter.bard.edu/files/2017/04/CSD-Drone-Incidents.pdf.

[113] *Id.*

infringement on U.S. citizens' privacy.[114] Section 5 of the FTC Act[115] (Act) grants the FTC the authority to prevent individuals and companies from committing "unfair or deceptive acts or practices," such as broken privacy and data security promises, as well as unfair collection of personal information.[116] The Act is the common consumer protection law for privacy in the United States.[117] Embodied in the Act are a set of principles, known as the Fair Information Practices (FIP), that regulate the relationship between business and government entities that collect, use, and disclose personal information about ordinary people.[118] The Act attempts to assure individuals that their data is being processed in a way that gives individuals notice and some choice about certain uses of their data.[119] The Act, along with other U.S. statutes, builds on the FIP principles.[120]

The United States' current approach to defining, governing, and protecting personal data triggers at least three concerns. First, the Act is not tied to the individual's rights over personal data, meaning the FTC is regulating the physical transaction instead of recognizing and protecting one's right to personal information.[121] Second, studies show that the FTC rarely comes into contact with businesses and government entities, and that when the FTC does, sanctions are generally limited to small fines and cases are often settled out-of-court.[122] Third, only the FTC can regulate this issue; there is no private right of action for individuals whose personal information has been wrongly collected.[123] Individuals

---

[114] *See Protecting Consumer Privacy and Security,* FEDERAL TRADE COMMISSION, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Mar. 31, 2021).

[115] Federal Trade Commission Act Section 5: Unfair or Deceptive Acts of Practices. A practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." Federal Trade Commission v. Wyndham Worldwide Corp., 799 F.3d 236, 244 (3d Cir. 2015). Further, an act or practice is unfair when it leads to a substantial consumer injury that consumers cannot prevent and is not outweighed by benefits to consumers or businesses. This again favors the business over the consumer. *See* Julia Whall, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of LABMD,* 60 B. C. L. REV. 149, 154 (2019).

[116] Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, 25 THE J. OF THE ANTITRUST, UCL & PRIVACY SEC. OF THE ST. B. OF CAL. 89 (2016).

[117] William McGeveran, *Friending the Privacy Regulators,* 58 ARIZ. L. REV. 959, 977 (2016).

[118] RICHARDS *supra* note 15, at 73.

[119] *Id.* at 74.

[120] The FIP is also at the foundation of OECD Guidelines and the 1995 EU Data Protection Derivate. *See id.*

[121] *See* McGeveran, *supra* note 117, at 977.

[122] Bob Sullivan, *'La Difference' is Stark in EU, U.S. Privacy Laws*, NBC NEWS (Oct. 19, 2006, 11:19 AM), http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.XbXAxpNKiL8.

[123] *See* McGeveran, *supra* note 117, at 979.

can file complaints with the FTC, but unlike EU authorities, the FTC has no obligation to act on these grievances.[124]

The issues surrounding U.S. regulation of data privacy is attributed to how the United States defines personal information. Personal information in the United States is often thought of as a person's name rather than the elements that make up a person's identity, as in the EU.[125] As a result, a data breach in the United States occurs when a breacher collects identifiable names in combination with non-public information such as a social security number.[126] This definition has allowed companies to get personally identifiable information about an individual and use that data for valuable purposes.[127] The specific requirements and narrow definition of personal information allows loopholes for many companies and individuals to collect personal information. Americans are much more willing to tolerate industry self-regulation as they see the economic value of consumer data; however, favoring the market and allowing all of these various common law regulations actually decreases the efficiency of the market.[128] If the U.S. government prioritized protecting privacy on the front-end, then companies could contractually manage privacy to increase efficiency and commercial growth.

One form of front-end privacy contracting occurred in the 1990s by requesting individual's consent for data collection. The concept of individual consent, however, no longer works in the age of big data.[129] Companies provide this individual consent in the form of multiple paragraphs of complex language in nine-point font followed by a check box. While people check the box, the consent is impartial since people rarely read or understand the policy agreed upon.[130] Further, this procedural protection does not actually protect substantive data privacy information like the EU model does.[131] Also, in the context of commercial drone usage specifically, one problem is that even if the person who ordered the package

---

[124] *Id.*

[125] Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 891 (2014).

[126] *Id.* at 889–90.

[127] *Id*. at 911.

[128] *See* Whitman, *supra* note 23, at 1192 (highlighting how "[t]rafficking in consumer data lowers search costs: It makes it easier for buyers and sellers to find each other, creating sales that would otherwise not have been made, and thereby enhances the efficiency of the market.").

[129] Cameron F. Kerry, *Why Protecting Privacy is a Losing Game Today—And How to Change the Game*, BROOKINGS (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/ (explaining that the idea of online consent came from medical cases where consent was often asked in person).

[130] *See id.* (noting that "[m]aybe informed consent was practical two decades ago, but it is a fantasy today. In a constant stream of online interactions, especially on the small screens that now account for the majority of usage, it is unrealistic to read through privacy policies. And people simply don't.").

[131] *See* McGeveran, *supra* note 117, at 978 ("[The U.S. model] does not provide individuals with the broad rights of access or correction they have under the data protection model.").

consents, the neighbor whose house the drone flies over and videos has not consented.[132]

Proposed regulations like the Consumer Privacy Bill of Rights (Privacy Bill)[133] have suggested solutions for these consent issues. Implicit in the Privacy Bill is the idea of protecting personal data and focusing protection on the company rather than the individual.[134] The Privacy Bill adopts a similar framework to GDPR, giving consumers a baseline of the rights that companies should respect. Moreover, the Privacy Bill acknowledges that "consumers have a 'right to secure and responsible handling of personal data,' and companies are expected to 'maintain reasonable safeguards' to control the risk of unauthorized access and improper disclosure."[135] Unfortunately, the Trump Administration did not adopt the Privacy Bill. In fact, Trump's Administration made attempts to undo some of the privacy initiatives from the previous administration.[136]

Yet, on the other hand, individual states have begun adding more protections. The California Consumer Privacy Act ("CCPA") of 2018 granted consumers greater control and visibility over their personal information.[137] The CCPA mimics many of the principles and policies found in GDPR, such as the right for individuals to request that companies tell them what personal information has been collected, as well as the right to request that the companies delete their personal information.[138] The CCPA also defines personal identity as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular

---

[132] *See* Kerry, *supra* note 129 ("[I]ndividual choice becomes utterly meaningless as increasingly automated data collection leaves no opportunity for any real notice, much less individual consent."); *see also,* Kaminski, *supra* note 109 ("[D]rone surveillance will often provide no visible notice to the watched party if the drone is high up in the sky.").

[133] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1–2 (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

[134] *Id.* at 5–6.

[135] Gregory Evans, *Regulating Data Practices: How State Laws Can Shore Up the FTC's Authority to Regulate Data Breaches, Privacy, and More*, 67 ADMIN L. REV. 187, 200 (2015) (quoting WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 19 (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.).

[136] Stephen Y. Chow, *Current Developments*, *in* DATA SECURITY AND PRIVACY IN MASSACHUSETTS Chapter 16.1 (2d ed. 2018).

[137] *California Passes Furthest Reaching Privacy Law to Date*, BAKERTILLY (July 2, 2018), https://www.bakertilly.com/insights/california-passes-furthest-reaching-privacy-law-to-date/ (granting consumers: (1) a right to know what information has been collected, (2) a right to know why it has been collected and who it is being shared with, (3) and a right to tell companies to delete that information or not share or sell the personal data).

[138] John Stephens, *California Consumer Privacy Act*, ABA (February 14, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/bcl/2019/201902/fa_9/.

consumer or household."[139] Additionally, the CCPA provides a limited private right of action with fines up to $750 per incident.[140] But again, the CCPA only applies to California and will likely be weakened by the U.S. government. How the Government reacts to the CCPA will impact the future of federal drone regulations.

IV. PROPOSAL FOR NEW UNITED STATES DRONE PRIVACY REGULATION

To move to the forefront of drone usage and privacy protection, Congress should create a single federal drone regulation that protects against the infringement of data privacy. While the U.S. prides itself on protecting the drone market and is taking some steps—like the implementation of the Proposed Remote ID Rule—U.S. commercial drone companies have a long, slow, and expensive process of building these drone operations.[141] They will have to anticipate what legal issues they might face in each state. In thinking about potential solutions, EU drone regulation should serve as a model to the U.S. and inspire adding certain legal structures that promote productive privacy protection.

A. Congress Should Create a Federal Regulation Governing United States' Commercial Drone Usage and Privacy Concerns

The most efficient solution involves Congress creating a single federal regulation to govern commercial drone usage and privacy concerns. Most U.S. drone regulations are already in the hands of the FAA, a strong instrument to implement this regulation. Given the current status of these federal regulations, or lack thereof, federal legislation that takes a universal step towards regulating privacy is unlikely.[142] Therefore, many scholars have argued for state common law regulations. Some arguments include the fact that states are most familiar with regulating privacy issues and have already begun to do so in the drone world.[143] Others point to the "experimentation" argument and the fact that states are more

---

[139] CAL. CIV. CODE § 1798.40(o)(1).

[140] CAL. CIV. CODE § 1798.150.

[141] Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72,438, 72,514 (proposed Dec. 31, 2019) [hereinafter Proposed Remote ID Rule].

[142] Regulations such as the Drone Aircraft Privacy and Transparency Act of 2013 and the Preserving American Privacy Act of 2013 have not seen any movement since 2013. Even regulations implemented this year that have allowed drones to fly at night and UPS to begin commercially using drones and the new remote ID system regulation do not implement any privacy restrictions. *See* Drone Aircraft Privacy and Transparency Act of 2013, *supra* note 79.

[143] *See* Kamisnski, *supra* note 109, at 67–68.

equipped to protect consumer privacy concerns.[144] Especially if one chooses to look at drone use as the tort of intrusion, then states are best equipped to deal with that issue.[145] Individual state regulation, however, leaves major loopholes in terms of protecting from data collecting through images and voice recordings.

Furthermore, drone regulations do not need more state experimentation because federal privacy regulations are already in place, such as the Electronic Communications Privacy Act. These regulations have created a framework for warrants and court orders that cover law enforcement surveillance.[146] Moreover, state experimentation already took place because multiple states have enacted a variety of drone regulations that deal with both commercial use and privacy concerns.[147] State experimentation has led to extremely inconsistent regulations, which increases the cost for companies trying to use drones throughout the country because they have to comply with each state's rules and exclusions.[148] Further, if any federal regulation were to pass, it would preempt the various state regulations in place.[149] Thus, it is time for federal regulation.

Given the amount of state laws on data privacy, as well as international companies' compliance with the GDPR, having a single federal rule is the optimal approach. Evidence shows that "more companies are seeing value in a common baseline that can provide people with reassurance about how their data is handled and protected against outliers and outlaws."[150] The benefits of having one uniform federal regulation include "(1) the prevention of a lock-in of poor privacy standards . . . ; (2) the creation of the preconditions for effective market . . . contributions to privacy protections; (3) and the termination of United States intransigence on the wrong side of ongoing negotiations with the European Union about trans-Atlantic transfers of personal data."[151]

---

[144] *See* Kevin Townsend, *State vs. Federal Privacy Laws: The Battle for Consumer Data Protection*, SECURITY WK. (Nov. 13, 2018), https://www.securityweek.com/state-vs-federal-privacy-laws-battle-consumer-data-protection (outlining the current debates over state and federal privacy regulations).

[145] *See, e.g.*, RICHARDS, *supra* note 15, at 68 (discussing a situation where someone was found liable under a state tort of intrusion law).

[146] *See* Kamisnski, *supra* note 109, at 65 (explaining how some federal drone regulation could work in tandem with state regulations).

[147] *See* WIS. STAT. ANN. § 942.10 (West, Westlaw through 2019 Act 186); FLA. STAT. ANN. § 934.50 (West, Westlaw through 2020 Legis. Sess.); OR. REV. STAT. § 837.380 (2014).

[148] Jonathan Olivito, *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, 74 OHIO ST. L.J. 669 (2013) ("The difference in legal standards between circuits and states has resulted in judicial confusion and varying degrees of privacy protection across the United States.").

[149] *See* Kamisnski, *supra* note 109, at 73 (noting that the Preserving American Privacy Act could be read to preempt state regulation of drone flight between states).

[150] *See* Kerry, *supra* note 129.

[151] Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1615–16 (1999).

Notably, federal regulations are more apt to protect businesses rather than consumers; thus, one suggested solution is to allow the state drone laws currently in place to create the core of future federal regulation.[152] For example, both California's drone law as well as their new data privacy law would provide a good basis for federal regulation. The CCPA includes many elements of the GDPR that are suitable for this expanding technology, while California's drone laws reference the physical invasion of privacy that the United States has been more comfortable implementing.[153] The Wisconsin drone law also references the reasonable expectation of privacy idea, a concept that the U.S. Supreme Court has contemplated many times.[154]

Based on some of the strong state laws already in place, another possible solution is to allow the U.S. Government to regulate the core of drone regulations and then have states implement their own laws that can give more protection. This solution stems from the concern that if the Government modeled federal legislation off of the CCPA or the GDPR, such legislation would receive major pushback from big businesses. Taking into account the fact that Congress usually accommodates big businesses, such legislation would likely result in a very watered-down privacy regulation.[155] Rishi Bhargava, co-founder of a cyber-security start up company stated that

> a combination of federal laws, . . . and state laws . . . would be an ideal combination to aim toward. While base level federal requirements would be very useful, state-level laws allow for states to adopt additional, stricter measures to protect individuals' data and hold data controllers/processors accountable.[156]

There is also the possibility of having states adopt a Uniform State Law, which would allow the consistency of a federal regulation while providing more state

---

[152] *See* Townsend, *supra* note 144 (explaining how state laws are more likely to reflect the wishes of consumers).

[153] *See* Assemb. B. 856, Chapter 521, Reg. Sess. (Cal. 2015) ("This bill would expand liability for physical invasion of privacy to additionally include a person knowingly entering into the airspace above the land of another person without permission . . ."); California Consumer Privacy Act Assemb. B. 375**,** Chapter 55, Reg. Sess. (Cal. 2018) ("[t]he bill would grant a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer . . . .").

[154] WIS. STAT. ANN. § 942.10 (West 2015); *see* Katz v. U.S., 389 U.S. 347 (1967) (establishing the reasonable expectation of privacy test); Florida v. Riley, 488 U.S. 445, 446 (1989) (holding that an individual lacked a reasonable expectation of privacy in his greenhouse because the greenhouse was partially exposed to aerial view); U.S. v. Jones 565 U.S. 400, 407 (2012) (refusing to apply the reasonable expectation of privacy test).

[155] Townsend, *supra* note 144.

[156] *Id.*

protection and flexibility. Implementing a Uniform Law does, however, run the risk of not being nationally adopted or enforced like a federal regulation.[157]

Of course, there are legitimate safety reasons for regulating drones in the airspace safety context, but this Note focuses solely on the privacy aspect. Regulating drones through a privacy lens does not overstep the FAA, as it is not an either/or choice on how to regulate drones. Although there are a litany of aviation safety and air traffic issues that this Note does not address, airspace safety regulations are no less important than privacy regulations in the drone world. However, only regulating aviation safety and air traffic neglects one of the huge effects of drone usage. All drone laws should incorporate regulations that protect the privacy of U.S. individuals.

Federal data regulation is becoming more of a possibility as U.S. businesses are beginning to comply with foreign data protection laws and states in the United States are enacting data privacy laws as well.[158] Dana Simberkoff, Chief Risk, Privacy and Information Security Officer at AvePoint, notes there is a strong chance

> that the U.S. will move forward with federal privacy legislation in one form or another. There has long been speculation that the need for a federal data privacy policy would finally be realized only after the 'perfect storm' occurred—which is what we see happening in the privacy landscape today.[159]

With data privacy protection regulation on the rise, drone regulations that inherit some of these protections can easily follow.

In promoting a single federal regulation that would not only regulate commercial drone usage but also regulate privacy issues, crafting a single regulation that necessarily provides a single definition for privacy would be difficult. In recently enacted EU drone regulations, the GDPR privacy protections protect the fundamental right of information privacy.[160] The United States, on the other hand, defines privacy in various ways. Numerous regulations are used to protect data privacy.[161] Thus, while there are certain laws that adequately protect various privacy

---

[157] *See Uniform Laws*, LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/uniform/index.html (last visited, Mar. 14, 2020) (explaining that most uniform laws are not adopted by all states and states often make their own variations when passing the uniform laws).

[158] Townsend, *supra* note 144.

[159] *Id*.

[160] Commission Delegated Regulation 2019/945 of 12 March 2019, O.J. (L 152/1). *See* EASA, *Civil Drones (Unmanned Aircraft)*, https://www.easa.europa.eu/easa-and-you/civil-drones-rpas (last visited Nov. 14, 2019) (showing a timeline for implementing the new regulation.

[161] Wagner, *supra* note 15.

interests, it is necessary to determine what type of privacy a drone regulation should protect.

B. Congress Should Regulate Drone Privacy to Protect Against Data Privacy Infringement

A federal drone regulation should prevent data privacy infringement. While the strongest privacy laws in the United States protect against intrusion into physical spaces,[162] physical regulation will only work to a certain extent in enforcing drone regulations.[163] For example, if drone regulations prevent unlawful intrusions, companies can contract around the regulations, giving 'notice' to and obtaining 'consent' from individuals—and potentially their neighbors—who order deliveries from these companies.

Physical drone intrusion, however, is not the primary issue. Drones are equipped with video camera and microphone technology that enables people to acquire information inside an individual's home, which U.S. law has normally treated as completely private. One legal scholar, Neil Richards, has defined this personal information as "intellectual privacy" that includes "protection[s] from surveillance or unwanted interference by others when we are emerged in the process of generating ideas and forming beliefs—when we're thinking, reading, and speaking with confidants before our ideas are ready for public consumption."[164] The idea of intellectual privacy moves from an intrusion tort to a broader idea, such as an invasion of privacy.[165] While fashioning a regulation that protects a person's privacy seems straightforward, the history of privacy as described above illustrates the difficulties in defining 'privacy' uniformly and, thus, what a privacy regulation should actually protect.

In forming a federal drone regulation, one question in particular presents itself: What is considered private? As shown, many struggle with separating the concept of physical privacy from the concept of information privacy. For example, if a drone videoed someone within their home while that drone was dropping off a package at a neighbor's house, that video would constitute an invasion of privacy. Yet, if a drone photographed a neighbor's pool while flying over that neighbor's backyard and subsequently used that data to send the neighbor pool-cover ads, the answer is not as clear. Similarly, the Supreme Court found an individual lacked a reasonable expectation of privacy in his greenhouse because

---

[162] *See* Whitman, *supra* note 23, at 1161–62.

[163] *See* RICHARDS, *supra* note 15, at 156 ("Invasion of privacy is a useful way of thinking about legal restrictions on secret surveillance or bugging, whether by other people, by the government, or by drones. But intrusion alone will not be enough to solve all of the problems of information collection and dissemination.").

[164] *Id.* at 95.

[165] *See id.* at 156–57.

the greenhouse was partially exposed to aerial view.[166] Therefore, a federal drone regulation requires uniformly conceptualizing 'privacy,' something that neither Congress nor the Court has yet to do.[167]

Moreover, drone regulations must account for the fact that drones are also equipped with GPS trackers and equipment that could scan the products in one's home, collecting personal information about an individual and their family members.[168] The EU regulations provide helpful examples regarding these concerns. The EU has substantially progressed in protecting data privacy, as EU privacy laws have always focused more on informational privacy than on physical privacy.[169] As technological advancements have led to non-physical privacy infringements, more people in the United States consider the issues of informational privacy. Many states, such as California with its CCPA, and U.S. companies having to comply with GDPR to conduct international business, have already accepted the concept of informational privacy and passed regulations to protect it.[170]

Thus, one solution would be for the United States to mirror the EU's GDPR itself at a federal level; however, this idea would not easily integrate into the U.S.'s segregated regulation system, and it would likely bring up many conflicting interests between businesses and consumers. So, rather than adopting GDPR entirely, this Note suggests adopting aspects of GDPR in a federal regulation that might assimilate more easily into the United States' current legal system. One aspect of GDPR the United States should adopt is the EU's categorization of commercial drone use under personal data protection.[171]

While the U.S. does not have a single federal data-protection regulation, categorizing drone privacy concerns as data privacy would be the most efficient way to cover all privacy issues. Additionally, the GDPR is based on the same fair information practice principles as the Consumer Privacy Bill of Rights; however, the EU applies a straightforward and knowledge-based approach to its regulation.[172] The U.S. federal drone regulation could mirror the GDPR by specifically laying out how companies should manage privacy and provide notice to consumers through transparency rules.[173]

---

166 Florida v. Riley, 488 U.S. 445, 446 (1989).

167 *See* Kyllo v. United States, 533 U.S. 27, 34–35 (2001); *see also* United States v. Jones, 565 U.S. 400, 419 (2012); Callahan-Slaughter, *supra* note 67, at 244–45.

168 Calo, *supra* note 110.

169 *See* Whitman, *supra* note 23, at 1161.

170 *See* California Consumer Privacy Act Assemb. B. 375**,** Chapter 55, Reg. Sess. (Cal. 2018); GDPR, *supra* note 63 (including heavy penalties for non-compliance for any business around the world that collects or processes EU resident data).

171 *Regulation of Drones: European Union*, *supra* note 101.

172 *See* Kerry, *supra* note 129.

173 *See* GDPR, *supra* note 63.

Other U.S. regulations have provided suggestions on how to implement drone regulations. For example, in the new Proposed Remote ID rule for drones, one section of the regulation discusses privacy concerns for drone users.[174] The Proposed Remote ID rule proposes limiting the collection of data to only specific and necessary information, namely notifying individuals of collection practices and contracting over information regarding the use, protection, and storage of data.[175] While this specific regulation states that the "concerns regarding the use of small UAS to collect information about individuals . . . [is] beyond the scope of the FAA's mission to ensure safety and efficiency of aviation operations . . . ," a commercial drone regulation could easily adopt similar transparency and collection limitation practices.[176]

A strong privacy regulation must provide notice. In the EU, GDPR has a transparency policy rather than a pre-ticked check-box system of notice.[177] Transparency in GDPR involves specific practical requirements for data controllers and processors regarding the information collected and communication with data subjects concerning their rights.[178] The "transparency obligations begin at the data collection stage and apply 'throughout the life cycle of data processing.'"[179] GDPR's transparency policy requires that the notice language be clear and puts responsibility on the organization—not the individual—to ensure each individual receives and consents to all of the information.[180]

Third party notice is not a concern under the EU regulations for two reasons. First, GDPR places the notice requirement on the organization.[181] Thus, if an organization collects or processes an individual's data, they must provide notice to that individual.[182] Second, the EU considers privacy a fundamental right and therefore videoing or collecting personal information of a third party is an unlawful infringement of the right to privacy.[183]

---

[174] Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72,438, 72,514 (proposed Dec. 31, 2019) [hereinafter Proposed Remote ID Rule].

[175] *Id.*

[176] *Id.*

[177] *See* Müge Fazlioglu, *Transparency and the GDPR: Practical Guidance and Interpretive Assistance from the Article 29 Working Party*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Dec. 14, 2017), https://iapp.org/news/a/transparency-and-the-gdpr-practical-guidance-and-interpretive-assistance-from-the-article-29-working-party/.

[178] *See id.* (explaining the format and language in which the GDPR requires companies to provide transparency).

[179] *Id.*

[180] *See id.* (stating the burden the GDPR puts on companies).

[181] *Id.*

[182] *Id.*

[183] *See Summary of Privacy Rules in EU*, DRONE RULES, https://dronerules.eu/en/professional/obligations/summary-of-privacy-rules-in-eu (last updated Jan. 24, 2018) (explaining the key rules required to operate a drone in the EU).

The general idea of transparency is present in the FIP as well as in other privacy regulations.[184] A U.S. model could adopt the idea of transparency but would still face the issue of third-party consent.[185] The main challenge in federal drone regulation is that the United States does not recognize privacy as a fundamental right.[186] One solution would be to put the notice and consent requirement on the organization to notify a third party that they collected or processed any personal information. For example, the unadopted Drone Privacy and Transparency Act included a requirement that commercial drone companies present a data collection statement specifying when, where, and how long drone surveillance would take place.[187] This statement would have provided transparency and given notice to third parties. Moreover, the Drone Privacy and Transparency Act required that all drones have drone radio frequency identification[188] to track the drones and help determine whether a tort had occurred.[189]

Further, the unadopted Consumer Privacy Bill of Rights incorporated a similar transparency idea. The Bill included a principle stating that "[c]onsumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data."[190] This statement mirrors the idea stated in GDPR that regardless of the type of business, all companies must adhere to basic privacy principles regarding the use of one's personal data. Requiring companies to respect basic privacy rights and consumer expectations indicates a shift from simply providing notice to providing more of a guarantee that consumers' personal information will not be used in an adverse manner.

While the possible solutions discussed above would likely provide the highest level of consumer protection, such regulations would likely receive major push back from big companies. Therefore, this Note suggests other solutions that may be less burdensome on companies. Instead of adopting the very stringent GDPR

---

184 *See* Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY FORUM, https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ (last updated Dec. 19, 2007) (describing the openness principle of the FIP).

185 While protecting privacy on the front end through regulation will likely involve push back from big corporations, this is still a better option as it will allow the corporations to adapt on the front end and not be bogged down with varying litigation on the back end.

186 *See* David H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. RES. L. REV. 831, 837 (1991) ("[T]he Supreme Court has never made a broad general finding of a constitutional right to privacy.").

187 *See* H.R. 1262, *supra* note 79.

188 The FAA has now officially proposed this regulation. *See* Remote Identification of Unmanned Aircraft Systems, 84 Fed. Reg. 72,438, 72,439 (proposed Dec. 31, 2019) ("[R]emote identification of UAS would provide airspace awareness to the FAA, national security agencies, and law enforcement entities. This information could be used to distinguish compliant airspace users from those potentially posing a safety or security risk.").

189 *See* H.R. 1262, *supra* note 79.

190 WHITE HOUSE, *supra* note 133.

and EU privacy regulations, one solution to regulate privacy in the drone world is to adopt certain guidelines that promote fair consumer protection practices and principles. Legal scholar Cameron F. Kerry suggests a "simple golden rule for privacy: that companies should put the interest of the people whom data is about ahead of their own."[191] If adopted as a principle, Kerry's rule would effectuate proper notice and collection practices that Congress could later incorporate into a drone regulation. This principle is already incorporated in other regulations and guidelines. For example, the Cybersecurity and Infrastructure Security Agency ("CISA") has adopted "best practices" for drone users regarding certain security and privacy risks and how to address those risks. Some of these practices include safe installation and use of software, secure communications in flight, secure storage and transfer of data, and sharing knowledge with others.[192]

Moreover, some agencies have also issued guidelines to specifically help international companies comply with GDPR and other privacy regulations.[193] The United States could incorporate such guidelines into a federal regulation. Because most global companies are already spending a significant amount of money to comply with EU laws, implementing guidelines in the United States would likely receive far less pushback.[194]

From these guidelines come specific regulations the United States can adopt. For example, the Electronic Privacy Information Center suggests a three-pronged regulation encompassing use limitation, data retention limitations, and transparency.[195] The Electronic Privacy Information Center regulations encapsulate

---

[191] Kerry, *supra* note 129 (comparing these privacy principles to the ideas inherent in Louis Brandeis and Samuel Warren's law review article).

[192] *See* Cybersecurity and Infrastructure Security Agency, *Cybersecurity Best Practices For Operating Commercial Unmanned Aircraft Systems (UASs)*, CISA, https://www.waterisac.org/system/files/articles/Cybersecurity%20Best%20Practices%20for%20Operating%20Commercial%20Unmanned%20Aircraft%20Systems%20Fact%20Sheet.pdf (last visited Jan. 10, 2020); Grant Guillot, *Proposed Foreign Drone Bans—Is There Another Way?*, COMMERCIAL UAV NEWS (June 15, 2020), https://www.commercialuavnews.com/security/proposed-foreign-drone-bans-is-there-another-way ("Fundamentally, this guidance underscores that a drone must be treated in the same way a business treats any mobile device—a powerful storage and transmission vehicle that may be connected to the organization's enterprise network.").

[193] *See* Hannah Edmonds-Camara et al., *U.S. Draft Human Rights Guidance for Exporters of Surveillance Technology*, COVINGTON (Oct. 2, 2019), https://www.globalpolicywatch.com/2019/10/u-s-draft-human-rights-guidance-for-exporters-of-surveillance-technology/#page=1; Ben Wolford, *GDPR Compliance Checklist for US Companies*, GDPR.EU, https://gdpr.eu/compliance-checklist-us-companies/ (last visited Jan. 10, 2020).

[194] *See* Jeremy Kahn et al., *It'll Cost Billions for Companies to Comply With Europe's New Data Law*, BLOOMBERG BUSINESSWEEK (Mar. 22, 2018, 1:01 AM), https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law.

[195] *See* Urban, *supra* note 3, at 43.

many of the principles discussed above, including stipulating what data a company can collect and the notice that they must give regarding that collection.[196]

While the various guidelines discussed above are a great start to implementing a proper regulation, violating the guidelines must result in actual penalties in order for the guidelines to have any effect on privacy protection. The Electronic Privacy Information Center notes a need for a private right of action in its proposed regulations.[197] For instance, GDPR incorporates a private right of action where individuals are able to claim "material or non-material damage" as a result of a breach of GDPR.[198] Some form of punishment is necessary to ensure companies comply with a regulation that promotes transparency and dependable privacy protection.

V. CONCLUSION

In determining the best option for creating U.S. drone regulations, the United States can simply adopt the GDPR and EU's new drone regulations; however, there are inherent differences in the definition and treatment of privacy between the EU and the United States, such that adopting EU regulations would not work in the current U.S. landscape. For example, freedom of speech is not a fundamental right in the EU as it is in the United States, and the EU maintains much more control over individual information.[199] Thus, from a U.S. perspective, U.S. privacy laws have been doing just what they were designed to do, keep the government out. Nevertheless, the government not only has more ways to gain control of information with the proliferation of technological advancements, but so does every large company and the individuals that run them. Thus, more regulation is needed to protect one's privacy.

Given the history of privacy in the United States, the privacy framework in the EU provides only certain features for a federal regulation in the United States. The United States has always viewed privacy from a more physical perspective, thus, to ensure that informational privacy is protected from drone data-collection technologies, the privacy protections included in any drone regulation should prevent infringements of informational privacy. In looking at data privacy, the

---

196 *See id*.

197 *See id.* ("Effective privacy laws dealing with drone activities . . . must have a structure for supervising and auditing to ensure that drone usage remains for proper purposes and does not infringe on civil liberties.").

198 Todd Ehret, *Data Privacy and GDPR at One Year, a U.S. Perspective. Part Two—U.S. Challenges Ahead*, REUTERS (May, 29, 2019, 11:24 AM), https://www.reuters.com/article/us-bc-finreg-gdpr-report-card-2/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-two-u-s-challenges-ahead-idUSKCN1SZ1US.

199 *See* RICHARDS, *supra* note 15, at 54, 68.

CCPA serves as a strong model for new drone regulations. The CCPA requires more transparency and protections for informational privacy. Using state laws as a model for federal drone regulation helps to ensure that the regulation contains strong consumer protections.

To balance consumer interests against those of the corporations, Congress could require corporations to follow a set of principles that promote transparency and universal treatment toward individual privacy. Congress could build off these principals or allow states to step in where more protection is deemed necessary. Some of the fundamental privacy principles include transparency in the collection and use of personal information and a private right of action for individuals. Furthermore, imposing sanctions and penalties for breaching such principles is imperative to ensure compliance.

Due to pressure from U.S. states like California as well as the EU, federal data privacy regulation is on the rise in the United States. There is also recent evidence of the FAA allowing commercial drone usage along with the new Proposed Remote ID rule indicating that federal drone regulation is also on the rise.

Yet, a specific federal privacy regulation passing seems doubtful. Instead, the FAA is making certain regulatory advancements, allowing drone flight at night and approving the use of drone delivery for particular companies. However, in every regulation, the FAA continuously reiterates that third party privacy is outside the scope of FAA enforcement.[200] Thus far, only individual states have regulated privacy in the context of drone usage, which suggests the FAA is not going to regulate this issue even though such regulation is needed.

While U.S. state discussions on drone privacy regulation is a step in the right direction, the United States needs consistent regulation across all fifty states. Accordingly, the FAA tackling privacy concerns is the best option going forward. The apparent likelihood of a federal data privacy law could increase the possibility of a federal drone regulation including privacy protections. Data privacy regulations, or any regulation that protects informational privacy, is best suited to address the many drone privacy infringement capabilities. The FAA will cover physical privacy infringement issues through the regulation of public airspace. These federal regulations can take the form of general guidelines to ease the push back from businesses and state law can follow up for more consumer protections, giving structure and consistency for all parties to rely on.

The United States has typically been on the forefront of commercial growth and technological innovation; yet, U.S. privacy law cannot seem to move beyond the four walls of one's home. Nevertheless, an understanding of informational privacy has only grown, as illustrated by the CCPA's passing and company compliance with GDPR. Given the current legal landscape, the United States has the

---

[200] *See, e.g.,* Proposed Remote ID Rule, *supra* note 141 ("In the 2016 Rule, . . . the FAA noted that privacy concerns were beyond the scope of the FAA's mission to ensure safety and efficiency of aviation operations in the airspace of the United States . . . .").

potential to effectively protect individuals' personal information against privacy infringements from commercial drone usage through uniform federal data privacy legislation. Thus, as technological advancements soar, privacy protections should soar as well.