THE EYE IN THE SKY DELIVERS (AND INFLUENCES) WHAT YOU BUY

Hadar Y. Jabotinsky[♦] *& Michal Lavi*[♣]

"I initially mistook its noisy buzzing for a weed-whacker on this warm spring day. After several minutes, I looked out my third-story window to see a drone hovering a few feet away"[*]

ABSTRACT

Imagine that you are at home, when suddenly a drone peers into your window, takes a picture of your wardrobe, familiarizes itself with your fashion preferences, or takes a picture of your kitchen table during dinner. The drone immediately transfers the picture to the commercial platform that operates it, such as Amazon or Uber. The platform in turn targets you with personalized advertisements for merchandise or food, in real time, customized to your lifestyle, at the time when you are most susceptible, manipulating you to make a purchase. How should the law react to this? And what if a drone were to collect information on private individuals in public using sophisticated cameras, sensors and facial recognition software? What if the platform that operates drones were to collect and use information on consumers and third parties? Should the law limit such invasions of privacy?

The use of drones is growing rapidly and their technological capabilities are growing exponentially. Drones differ from existing surveillance technology. Their low cost and their ability to fly, equipped with high-resolution cameras, recording systems and sensors, enable them to take in information over longer periods of time and much more effectively than the human eye or ear. Such capabilities are liable to give rise to pervasive surveillance of a kind never known before. Making matters worse, invasion of privacy has serious consequences. By using a network of drone fleets at the service of a single commercial platform, such surveillance could allow the platform to effectively aggregate and analyze tremendous amounts of high-quality information on the parties under surveillance, gain valuable insight on consumers and influence their decisions to order merchandise or food.

[♦] Ph.D.(Law & Economics) Research Fellow, The Hadar Jabotinsky Center for Interdisciplinary research of Financial Markets, Crises and Technology; Research Fellow School of Law, Zefat Academic College.

[♣] Ph.D. (Law); Research Fellow, The Hadar Jabotinsky Center for Interdisciplinary research of Financial Markets, Crises and Technology; Research Fellow School of Law, Zefat Academic College.

We thank Emily Cooper for her invaluable input. We further thank the participants of the 2021 U.S. National Business Law Conference (U. Tennessee, June 2021). Special thanks are due to Simone Hunter-Hobson, Amani M. Carter, Vincent Cahill, George Frank, Daniella Cass, Alexander Burger, Sara Reeves, Jess Zalp, Mikaela Cordasco Jon Reid, Natalie Reynolds and their colleges on the *U. Pa. J. of Const. L.* staff for their helpful comments, suggestions, and outstanding editorial work that profoundly improved the quality of this Article.

This Article is dedicated to the memory of Michal's mother—Aviva Lavi—who died suddenly and unexpectedly. She will always be loved, remembered, and dearly missed.

[*] Rebecca J. Rosen, *So This is How it Begins: Guy Refuses to Stop Drone-Spying on Seattle Woman*, ATLANTIC (May 13, 2013) http://bit.ly/3bH0I1Q [https://perma.cc/U9FD-3ZU9].

While much of the scholarship on drone surveillance and invasion of privacy focuses on governmental use and the Fourth Amendment, this Article focuses on the use of drones by private entities engaged in commercial deliveries. Drone deliveries are relatively new; only a few companies have recently overcome the regulatory obstacles to receive Federal Aviation Administration approval for U.S. deliveries. COVID-19 has pushed companies to utilize drones for deliveries and has increased demand for it. Since drones are unmanned, they can deliver food and other products without close contact with the recipient. Such delivery can be safer, faster, cheaper and more efficient than traditional emissaries; yet alongside the benefits, the use of delivery drones can lead to invasion of privacy and can result in abuse of personal data for manipulation, raising significant challenges.

This Article addresses the challenges drones pose to privacy and proposes solutions. It aims to contribute to the literature in several ways. First, it outlines a roadmap of the different types of invasion of privacy and harm that can be caused by drones. It demonstrates that the physical boundaries of invasion no longer matter in light of advanced technology. In identifying types of invasion and harm, this Article takes the first step towards creating a legal policy for delivery drones. Second, this Article addresses existing law, arguing that currently there is a gap between the capacity of drones to observe and aggregate personal information and privacy protections under U.S. law. Third, it proposes solutions under privacy law, and even a duty of loyalty for platforms that operate drones. Finally, this Article accounts for possible First Amendment objections to the proposed solutions.

INTRODUCTION

In June 2019, Amazon's CEO of Worldwide Consumer business, Jeff Wilke, announced that the company expected to begin delivering packages via drone within months.[1] Amazon received Federal Aviation Administration (FAA) approval to operate its fleet of Prime Air delivery drones, designed to safely convey packages to customers in 30 minutes or less.[2] FAA approval allows the company to expand unmanned package delivery.[3] Amazon is a pioneer in the field of drone delivery and commenced pilot testing for their Prime Air project of drones in 2016.[4] Yet Amazon is not the only company seeking to expand drone deliveries. Alphabet-owned Wing is the first drone delivery company to receive FAA approval for commercial deliveries in the U.S.[5] Uber plans to incorporate Unmanned Aerial Vehicle (UAV) delivery into its Uber Eats food-delivery business by

1 *From Retailers To Insurance Providers, Here Are 21 Corps Using Drone Tech Today*, CB INSIGHTS RSCH. REPORT (June 26, 2019), https://bit.ly/32fN4gs [https://perma.cc/V39G-DWM].

2 Annie Palmer, *Amazon Wins FAA approval for Prime Air Drone Delivery Fleet*, CNBC (Aug. 31, 2020, 9:48 AM), www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html [https://perma.cc/54V2-REZN].

3 Megan Cerullo, *Amazon Delivery Drones Receive FAA Approval*, CBS NEWS (Sept. 2, 2020, 11:25 AM), cbsn.ws/3kloTTT [https://perma.cc/7VA8-PZVS].

4 Alex Hern, *Amazon Claims First Successful Prime Air Drone Delivery*, THE GUARDIAN (Dec. 14, 2016, 10:02 AM), https://www.theguardian.com/technology/2016/dec/14/amazon-claims-first-successful-prime-air-drone-delivery [https://perma.cc/76GM-LJ3Q].

5 Jon Porter, *Alphabet's Wing Drones Get FAA Approval To Make Deliveries In The US*, THE VERGE (Apr. 23, 2019, 12:13 PM), https://www.theverge.com/2019/4/23/18512658/google-alphabet-wing-drone-delivery-service-faa-approval-commercial-deliveries [https://perma.cc/ZF7D-N5XM].

2021 and has already tested the service.[6] Walmart, the American retail corporation, is now piloting on-demand drone delivery using automated drones by end-to-end drone delivery company Flytrex.[7] Walmart expects to gain valuable insight into customers by using drones for delivering groceries.[8] More and more commercial industries are discovering the benefits of drone deliveries.[9]

Drones, or unmanned aerial vehicles, have been used by the military for remote surveillance since World War I.[10] Until a decade ago, drones were used mostly by the military.[11] Yet a revolution has occurred in American society and today there are approximately 2,000,000 drones in operation, extending far beyond military use.[12] Drones are now used for commercial purposes, enhancing public safety, improving science, law enforcement and more.[13] Much of the attention regarding drones focuses on government use, for example for law enforcement purposes, for obtaining a view of crime scene,[14] and for monitoring protests;[15] yet this Article will focus on civilian commercial use of drones for delivery purposes. Such drones offer "a market opportunity that is too large to ignore" for manufacturers and investors.[16] The use of commercial drones for delivery purposes is particularly promising.

---

6 Associated Press, *Uber Test Uses Drones To Deliver McDonald's Meals*, CHICAGO TRIBUNE (June 13, 2019, 3:40 PM), bit.ly/32haCSa [https://perma.cc/FGX4-J727].

7 Press Release, *Walmart Now Piloting On-Demand Drone Delivery With Flytrex* ,sUAS News (Sept. 10, 2020), bit.ly/34ZIk0n [https://perma.cc/W5NA-HTR2].

8 *Id*.

9 *From Retailers To Insurance Providers*, *supra* note 1. *See, e.g.*, Julianne Pepitone, *Domino's Tests Drone Pizza Delivery*, CNN TECH (June 4, 2013, 6:29 PM), https://money.cnn.com/2013/06/04/technology/innovation/dominos-pizza-drone/index.html [https://perma.cc/GD4E-DYCE].

10 Kashyap Vyas, *A Brief History of Drones: The Remote Controlled Unmanned Aerial Vehicles (UAVs),* INTERESTING ENGINEERING (June 29, 2020) https://interestingengineering.com/a-brief-history-of-drones-the-remote-controlled-unmanned-aerial-vehicles-uavs [https://perma.cc/YR8ZzPKSF].

11 Nikki J. Stehr, *Drones: The Newest Technology for Precision Agriculture,* 44 NATURAL SCIS. EDUC. 89 (2015).

12 Steve Calandrillo, Jason Oh & Ari Webb*, Deadly Drones? Why FAA Regulations Miss the Mark on Drone Safety,* 23 STAN. TECH. L. REV. 182, 195 (2020).

13 *Id.*

14 *Street-Level Surveillance: Drones/Unmanned Aerial Vehicles,* ELEC. FRONTIER FOUND., https://www.eff.org/pages/dronesunmanned-aerial-vehicles [https://perma.cc/W58DKA2Z].

15 *See, e.g.*, John D. McKinnon & Michelle Hackman, *Drone Surveillance of Protests Comes Under Fire*, THE WALL STREET JOURNAL (June 10, 2020, 3:47 PM), https://www.wsj.com/articles/drone-surveillance-of-protests-comes-under-fire-11591789477 [https://perma.cc/C5AG-6CVL].

16 *Drones: Reporting for Work*, GOLDMAN SACHS (2019) (last visited Feb. 11, 2022, 10:13 PM) https://www.goldmansachs.com/insights/technology-driving-innovation/drones/ [https://perma.cc/4YEW-FC9K].

Drone operating costs are low relative to other aerial vehicles.[17] Drone use is cheaper than other shipping methods and can also reduce labor costs.[18] Drones can deliver packages to remote areas faster than traditional emissaries.[19] Because drones do not rely on road infrastructure, they can bypass increasing traffic jams and deliver packages by the optimal route, fulfilling consumers' ever-growing demands for shorter delivery times.[20]

However, despite the obvious benefits, delivery drones are not yet widespread in the U.S. due to regulatory challenges, which currently constitute the most prominent obstacle to use.[21] Federal Aviation Administration (FAA) regulations, which aim to enhance safety, also limit the potential of drone technology.[22] Beyond the FAA requirement that all drone operators register their personal information with the Federal Government, a requirement that is not likely to impede commercial drone use,[23] FAA rules have instituted a "line of sight" requirement.[24] This requirement forbids flying drones outside the natural field of vision of the operator, who must be able to view and maneuver the drone to avoid hazards.[25] This regulation has been heavily criticized in literature for stifling innovation in drone technology

---

17 *See* Seyed Mahdi Shavarani et al., *Application of Hierarchical Facility Location Problem for Optimization of a Drone Delivery System: A Case Study of Amazon Prime Air in the City of San Francisco,* INT. J. ADV. MANUF. TECH. (2018) ("The carbon fiber used in drones is now cheaper which results in cheaper prices of drones.")

18 *See* Stanislav Ivanov et al., *Adoption of robots and service automation by tourism and hospitality companies*, 27 REVISTA TURISMO & DESENVOLVIMENTO 1501, 1510 (2017) ("[O]ver 150 guests at the OppiKoppi music festival in South Africa received cold beer via drone, giving the recipients the convenience of delivery while cutting down on the labor cost of delivery.")

19 *See* Linda Grandstein, *Pie in the sky: Israeli Startup's Drones Deliver to Your Backyard in 15 Minutes*, THE TIMES OF ISRAEL (Dec. 27, 2021) https://www.timesofisrael.com/spotlight/pie-in-the-sky-israeli-startups-drones-deliver-to-your-backyard-in-15-minutes/ [https://perma.cc/S63P-LQ28] ("Flytrex CEO Yariv Bash says drone delivery is cheaper, faseter and safer than traditional delivery.").

20 *See* Jinsoo Hwang & Ja Young (Jacey) Choe, *Exploring Perceived Risk in Building Successful Drone Food Delivery Services*, 31 INT J. CONTEMP. HOSP. MANAG. 3249, 3251 (2019); Sarah Lyon-Hill et al., *Measuring the Effects of Drone Delivery in the United States,* VIRGINIA TECH. REPORT (Sept. 2020) (finding that drone delivery presents the capacity to reduce vehicle traffic, CO_2 emissions, and road accidents); Ngui Min Fui Tom, *Crashed! Why Drone Delivery Is Another Tech Idea Not Ready to Take Off*, 13 INTL. BUS. RES. 251, 256 (2020) ("The use of Drone was a convenient and efficient technology for delivery services as it shortened the delivery time to as low as 30 minutes and delivers the merchandise to consumer's doorstep[.]").

21 Calandrillo, supra note 13, at 186

22 Calandrillo, *supra* note 13, at 186 (asserting that the regulatory requirement to register personal information with the federal government needlessly restricts the productive use of drones).

23 49 U.S.C. § 44807 (2018); 14 C.F.R. § 107.13 (2019); Calandrillo, *supra* note 12, at 187.

24 Calandrillo, supra note 13, at 186.

25 14 C.F.R. § 107.31 (2019); Calandrillo, *supra* note 12, at 191.

and reducing the social utility of drone usage.[26] Most commercial and revenue-producing opportunities that would provide added value, such as long package delivery, would be beyond the visual line-of-sight (hereinafter: BVLOS).[27]

Opponents of this regulation claim that stifling innovation with the line-of-sight requirement is unnecessary for ensuring safety and is based on a misperception of risk.[28] Because cameras and collision-avoidance technology autonomously sense, detect, and avoid obstacles from all angles, drone operators do not need to visually see their drones in order to prevent collision. Manufacturers today are more than capable of installing high-resolution cameras into drone cockpits, which transmit a live, "first person view" feed to their operator.[29] Moreover, drones now have the technological capacity to autonomously detect and avoid objects from all angles.[30]

Currently the FAA allows some drones to operate in the U.S. BVLOS.[31] As it stands, the FAA requires most drone operators to obtain waivers to fly BVLOS.[32] However, obtaining this waiver is "cumbersome and can take three to six months, which is longer than most innovative companies can afford to wait."[33] Furthermore, in 2018, only 16% of all 11,325 applications reviewed received approval.[34] Drone experts believed it would take years before all delivery drones would be allowed to fly freely BVLOS on a large scale.[35] However, more companies are overcoming the regulatory obstacles

---

26 *See* Calandrillo, *supra* note 12, at 230 ("…instead, the FAA's line-of-sight and drone registration requirements work primarily to suffocate innovation in drone technology and reduce the social utility of drone usage.")

27 *See* John Villasenor, *Observations From Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J. L. & PUB. POL'Y 457, 466 (2013) (explaining that regulation that does not permit UAS flights in which the operator on the ground is unable to maintain continuous visual contact with the aircraft hinders long distance drone flights).

28 Calandrillo, *supra* note 12, at 230.

29 *Id*. at 231.

30 *Id*. at 232.

31 Calandrillo, *supra* note 12, at 236; *see also* Ed Oswald, *Here's Everything You Need To Know About Amazon's Drone Delivery Project, Prime Air*, DIGITAL TRENDS (May 3, 2017), https://www.digitaltrends.com/cool-tech/amazon-prime-air-delivery-drones-history-progress/ [https://perma.cc/PGT7-84MV].

32 Dawn Zoldi, et al., *Drone Law and Policy*, 17 SCITECH LAWYER CHI. (2021) ("[T]he FAA still views BVLOS operations with caution. As mentioned, to fly BVLOS, a small drone operator requires a Part 107 waiver.")

33 Calandrillo, *supra* note 13, at 236.

34 *Id*.

35 Steven De Schrijver, *Commercial Use of Drones: Commercial Drones Facing Legal Turbulence: Towards a New Legal Framework in the EU*, 16 US-CHINA L. REV. 338, (2019) (estimating that three to four years

to drone delivery and it seems that widespread use of delivery drones is closer than ever. [36]

Beyond regulatory hindrances, there were other causes for the slow adoption of delivery drones, the first being technological: small drones generally have short flight duration capacity.[37] However, new developments in drone technology, such as solar-powered drones[38] and expanded battery life, are expected to result in more extensive use of drones for deliveries.[39] Another reason for slow adoption is that at first, consumers might be reluctant to select the drone delivery option because it is unfamiliar and they may be concerned about the security of drone deliveries and vulnerability to exploitation by hackers.[40] Consumers might also be uncertain of financial risks that might arise when drone delivery services do not perform as expected, or be concerned that navigating the new system would require effort and be a waste of time.[41] Despite consumer concerns, eventually they are likely to adopt drone deliveries, just like many other innovations.[42] The early adopters will be the first to use drone deliveries. Subsequently, the early majority and the late majority will follow. Finally, the laggers will see that drone deliveries are widespread and they will follow suit.[43]

COVID-19 has pushed society and the government to reconsider, better understand, and increasingly utilize drone innovation.[44] Due to the social distancing guidelines imposed because of the virus, the demand for drone

---

would be required before delivery drones would be able to fly beyond the visual line of sight of the drone operator and achieve their maximum potential).

36 *See, e.g.*, Palmer, *supra* note 2 (identifying Amazon, Alphabet, and the UPS as companies that secured FAA approval to operate drone fleets for commercial purposes).

37 Big Alin, *Why Do Drones Have Short Flight Times? And How To Get More*, DRONESVUE https://dronesvue.com/why-do-drones-have-short-flight-times/ [https://perma.cc/W35Q-5VQG].

38 *See* Villasenor, *supra* note 27 (noting that solar-powered UAVs can stay aloft for "extraordinary periods of time" ranging between two weeks and five years).

39 *See* Calandrillo, *supra* note 13, at 237 ("Google overcame hurdles to perfect drone delivery by extending drone battery life for long distance deliveries[.]").

40 *See* Hwang & Choe, *supra* note 20, at 3253 (specifying credit card numbers and phone numbers as susceptible to exposure and misuse).

41 *See* Hwang & Choe, *supra* note 20, at 3252 (noting that where consumers have difficulties navigating a new system, their time is likely to be wasted and their product or service receipt may be delayed).

42 Wonsang Yoo et al., *Drone Delivery: Factors Affecting the Public's Attitude and Intention to Adop*t, 35 TELEMATICS AND INFORMATICS 1687 (2018).

43 *See* EVERETT M. ROGERS, DIFFUSION OF INNOVATION 27 (5th ed. 2003) (explaining the process of diffusion of innovation).

44 *See* Ngui Min Fui Tom, *supra* note 20 (listing the companies that have received certification for commercial drone delivery services).

deliveries is expected to grow.[45] The FAA is likely to grant more approvals to commercial companies to use delivery drones and companies are likely to find innovative solutions for technological and security problems.[46] Moreover, consumers now have more powerful incentives to adopt them. Thus, we should expect to see more and more delivery drones overhead in the near future.

The use of delivery drones has many benefits. However, there is a flip side as drone deliveries can lead to substantial invasion of privacy, giving rise to a level of pervasive surveillance never seen before. Drones have the ability to reach and observe places other aerial platforms were unable to observe,[47] and their cameras enable high-resolution photography far beyond the capacity of the naked eye. It is thus easy for drones to obtain imagery that includes "intimate details."[48] Moreover, drones can be equipped with facial recognition technology that can enable operators to recognize people in their homes or on the streets.[49] Drones can also be equipped with recording systems that allow them to record conversations from afar, way beyond the capacity of the unaided ear. Recording technologies create a permanent record, taking in more information over a much longer period of time. Such technologies could allow drones to collect highly sensitive information.

Commercial delivery drones operate for platforms that sell merchandise or food. A network of drone fleets never sleeps, blinks, gets confused, or loses its attention span. It aggregates information on various consumers that can be combined, analyzed, and used to reach conclusions about consumers who order merchandise or food. In turn, platforms that operate drones, such as Amazon, can gain valuable insight into consumer personalities and desires, providing them with immediate feedback on what consumers are doing, or plan to do, and enabling them to target consumers with messages in ways

---

45 *See* David Street, *Online Food Platforms Set to Grow Despite the Pandemic*, SUCCESS (May 5, 2020), bit.ly/3keaclE [https://perma.cc/9RZM-2SUZ] (identifying Uber as one company exploring the viability of delivery drones for food delivery).

46 Lyon-Hill, *supra* note 20.

47 Wells C. Bennett, *Civilian Drones, Privacy, and the Federal-State Balance*, BROOKINGS (Sept. 2014), https://www.brookings.edu/research/civilian-drones-privacy-and-the-federal-state-balance/ [https://perma.cc/N8BX-Z4U4].

48 Villasenor, *supra* note 27, at 494.

49 *See* Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC (July 5, 2020), bit.ly/3n6DzYR [https://perma.cc/P6DC-SR2P] ("In the past few weeks, Homeland Security has spied on protesters in 15 cities using drone surveillance, while police body cameras equipped with facial-recognition technology have captured images of protesters.").

that were previously impossible. In doing so, these platforms can influence and even manipulate consumer decisions to order products.[50]

The unique ability of drones to easily and inexpensively obtain observations from above, by using imaging cameras and other information gathering capabilities, places them at the complex intersection between technology and privacy.[51] New technology presents challenging and divisive privacy issues. As early as 1890, Warren and Brandeis recognized the threat of newly invented cameras capable of taking "instantaneous photographs" and the ability of those cameras to invade "the sacred precincts of private and domestic life."[52] Warren and Brandeis concerned themselves with the "numerous mechanical devices that threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[53] In their seminal law review article, *The Right to Privacy*, they recognized that "the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to redefine the exact nature and extent of such protection."[54]

As more and more technologically advanced drones soar in the sky, the likelihood that individual privacy might be violated by this "eye in the sky" will come to pose a greater risk. Currently, the law regarding invasion of privacy lags behind technology and is insufficient to protect individual privacy against invasion and misuse of data through modern drone technology.[55] This Article aims to narrow this gap, and is structured as follows:

Part I defines commercial drones and their benefits. Subsequently, it addresses invasion of privacy and outlines a roadmap of delivery drone privacy invasions and the harm they inflict, focusing on: (1) trespassing on private property, (2) looking from afar, (3) surveillance in public, and (4) collecting and analyzing personal information. It demonstrates that due to technological developments, the traditional separation between privacy at

---

50 See SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (coining the term "surveillance capitalism" and explaining its impact on commerce, free will and society).

51 Villasenor, *supra* note 27, at 459.

52 Rebecca L. Scharf, *Drone Invasion: Unmanned Aerial Vehicles and the Right to Privacy*, 94 IND. L.J. 1065, 1069 (2019).

53 *Id.*

54 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

55 Scharf, *supra* note 52, at 1067.

home and in public collapses, and therefore there is a need to propose a new balance between technology benefits and privacy costs.

Part II overviews current common legal regulation against invasion of privacy. Next, it argues that current U.S. law is ill-equipped to accommodate invasions of privacy caused by drone delivery, as it lags behind technology that enables drones to extensively expose intimate details even in public spaces, as well as to aggregate personal information. Moreover, current U.S. law focuses on privacy as freedom from intrusion and the freedom to exclude the public and neglects to address the consequences of such intrusions. Thus, it provides insufficient privacy protections against invasion of privacy resulting from drone delivery.

Part III calls for a new regulatory framework that would expand privacy protections and provide a better balance between proliferating technology and privacy costs. Such a framework should consider not only the invasion of privacy caused by delivery drones themselves, but rather pose limitations on data collection, misuse and retention by the platforms operating drones. Policymakers can learn from the EU's General Data Protection Regulation,[56] and other EU legislation regulating commercial drone use.[57] A supplementary framework can be set forth by adopting a duty of loyalty[58] or a similar fiduciary model of privacy,[59] which would change the conditions for platform surveillance capitalism and data opportunism.

Part IV concludes by addressing First Amendment objections regarding the constitutionality of the proposed delivery drone regulation framework.

---

56 Regulation 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) [hereinafter GDPR].

57 Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency.

58 Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law* (July 3, 2020), papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217.

59 Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 16 (2020).

I. UP IN THE SKY: WHAT ARE DRONES? DELIVERY DRONES, THEIR BENEFITS AND PRIVACY RISKS

A. What are Drones? Definitions and Types

Look! Up in the sky! It's a bird . . . it's a plane . . . it's a drone![60]

A drone is defined as a small, unmanned aircraft with the capacity to fly autonomously, operating without a pilot on board.[61] Early drone prototypes were often used for military purposes and later on for other state or federal public uses.[62] As technology developed, the use of drones expanded to civilian use by private companies, individuals, and other non-governmental entities.[63]

Drones can be operated by a human pilot from a distance, and that is the only type of drone generally permitted by regulations.[64] In addition, some drones are automatically programmed, without being operated or controlled by a human. Such Unmanned Aircraft Systems ("UAS") are not yet authorized for use by the International Civil Aviation Organization (ICAO) of the UN, or under EU rules.[65] In the U.S. there is no explicit prohibition against UAS, yet there is an implicit restriction on their use, since their use is subject to the issuance of experimental certificates.[66] Since 2017, the U.S. Department of Transportation (USDOT) and the FAA have been evaluating their integration into the national airspace system and formulating new rules to support their operation.[67]

---

60 *See Superman* (Fleischer Studios 1941) ("Look! Up in the sky! It's a bird . . . it's a plane! It's Superman!").

61 Jason Snead & John-Michael Seibler, *Redefining "Aircraft," Defining "Drone": A Job for the 115th Congress*, 197 HERITAGE FOUND., 1–8 -8 (2017). *See also* De Schrijver, *supra* note 35, at 339 (referring to the memo of the European Commission (2014) that uses the term drones to describe any type of aircraft that is automated and operates without a pilot on board); European Commission Memorandum 14/259, Remotely Piloted Aviation Systems (RPAS)—Frequently asked questions (Apr. 8, 2014), http://europa.eu/rapid/press-release_MEMO-14-259_en.htm [https://perma.cc/EC6Y-8DKB].

62 Calandrillo, *supra* note 13, at 194–95.

63 Hwang and Choe, *supra* note 20, at 3250.

64 *See* De Schrijver, *supra* note 35, at 339 (referring to the E.U regulation); *see also* Calandrillo, *supra* note 13, at 191 (referring to U.S FAA Regulation that "requires that all commercial drone operators obtain a remote pilot certificate").

65 De Schrijver, *supra* note 35, at 339.

66 14 C.F.R. § 21.191 (2002). The list in § 21.191 includes purposes such as "[r]esearch and development," "[a]ir racing," and "[c]rew training," but it does not include commercial use.

67 *UAS Integration Pilot Program*, FED. AVIATION ADMIN. (last modified Dec. 17, 2021), https://www.faa.gov/uas/programs_partnerships/completed/integration_pilot_program/ [https://perma.cc/GCF2-3XWV].

Drones are astonishing technological advancements.[68] Not only can they reach new physical heights and limits, but they can also record a vast amount of information through photography, live video feeds, and sophisticated sensors, including location information, audio, thermal imaging, facial recognition, night vision, and data interception.[69]

The vast capabilities described above are ever-increasing due to technological advancement and they can enable industries to use drones for diverse innovative purposes at a relatively low cost.[70] For example, journalists can use drones to quickly reach otherwise inaccessible areas, and provide imagery from different angles.[71] Farmers can use drone technology to improve agricultural capabilities and maximize crop efficiency by allowing "planning and strategy based on real-time data gathering and processing" which provides farmers with information on precisely when to irrigate or apply fertilizers to crops.[72] Drones also hold promise in the construction industry: "With a bird's-eye view of construction sites, allowing them to monitor site progress, detect early structural defects, and identify potential hazards and quality concerns."[73] The insurance industry also stands to benefit from drones that could help improve risk management.[74] Other industries that might benefit from drones include the marketing industry, which could use visual content from drones for marketing[75]; the entertainment industry, which could employ drones for filming[76]; the real estate marketing industry, which could use them to provide potential buyers with information and details on the area surrounding the property[77]; the tourism industry, which could use drone photos to attract tourists[78]; and the medical industry, which is starting to use them to deliver medical equipment, and transport samples and tests from one place to another.[79]

---

68 Scharf, *supra* note 52, at 1070.

69 Scharf, supra note 52, at 1070.

70 *Id.* at 1073.

71 Calandrillo, *supra* note 13, at 195.

72 *Id.* at 198–99.

73 *Id.* at 200.

74 *Id.* at 202.

75 *Id.* at 204.

76 *Id.* at 205.

77 *Id.* at 206.

78 *Id.* at 208.

79 Harry Kretchmer, *How Drones are Helping to Battle COVID-19 in Africa – and Beyond*, WORLD ECON. FORUM (May 8, 2020), https://www.weforum.org/agenda/2020/05/medical-delivery-drones-coronavirus-africa-us/ [https://perma.cc/78TK-2553].

Drones can benefit a multitude of industries.[80] Yet the focus of this Article is on commercial drone delivery of merchandise and food, which is expected to increase sharply and become widespread. The first commercial drone delivery was approved by the FAA and took place on July 17, 2015.[81] Shortly afterwards, large corporations and businesses such as Amazon,[82] Alphabet (Google),[83] Walmart[84] and others started developing their own drone delivery services, and received FAA approval for their operations.[85] Thus, it is conceivable that in the near future drones could augment or replace the fleets of trucks previously operated by companies.[86]

B. The Sky is the Limit: Drone Delivery Benefits

Drones have truly disruptive potential and can be a game changer in the industry of delivery services, due to benefits never known before. As the following subsections explain, delivery drones are superior to traditional emissaries in several ways.

First, drone deliveries are fast and efficient. They can deliver packages to remote rural areas[87] without dependency on road infrastructure. They can also bypass traffic jams and deliver packages by the optimal route,[88] reducing unnecessary travel and save time.[89] For example, Amazon Prime Air Project, which has yet to materialize,[90] intends to use autonomous drones to fly individual packages to customers within 30 minutes of ordering. Another

---

80 Calandrillo *supra* note 13, at 209–19 (overviewing more private and public beneficial applications of drones demonstrating that their use can even save lives).

81 Mike Murphy, *The First Successful Drone Delivery in the US has Taken Place*, QUARTZ NEWS (July 20, 2015), https://qz.com/458703/the-first-successful-drone-delivery-in-the-us-has-taken-place/ [https://perma.cc/5ABU-ZVCM].

82 Cerullo, *supra* note 3.

83 Porter, *supra* note 5.

84 *Walmart Now Piloting On-Demand Drone Delivery With Flytrex*, *supra* note 8.

85 Cerullo, *supra* note 3.

86 Therese Jones, INTERNATIONAL COMMERCIAL DRONE REGULATION AND DRONE DELIVERY SERVICES, RAND CORP (2017), bit.ly/32zVz5Z [https://perma.cc/S4SQ-N4N3].

87 *See* Shiva Ram, Reddy Singireddy & Tugrul U. Daim, *Technology Roadmap: Drone Delivery – Amazon Prime Air*, INFRASTRUCTURE & TECH. MGMT. 387, 396 (2018) ("Once the drones have the efficient battery and power supply that lasts for longer times, it will be possible to deliver to remote areas as well.").

88 Hwang and Choe, *supra* note 20, at 3251; Ngui Min Fui Tom *supra* note 20, at 256 (discussing how "[t]he use of Drone was a convenient and efficient technology for delivery services as it shortened the delivery time to as low as 30 minutes and delivers the merchandise to consumer's doorstep, which in turn increased consumers' productivity and flexibility in daily life").

89 Lyon-Hill, *supra* note 20.

90 *See* Wikipedia, *Amazon Prime Air*, http://en.wikipedia.org/wiki/Amazon_Prime_Air [https://perma.cc/8QWU-GRD] (as of Feb. 25, 2021).

aspect of efficiency is allowing the customer real time information on the delivery. Moreover, the destination can be adjusted in real time, as the drone can follow the customer and deliver the package to any destination, even while the customer is on the go.[91] *Second*, drones are cheaper than other shipping methods and can reduce labor costs.[92] Drone delivery services also allow companies to integrate their supply chain and reduce shipping costs. For example, Amazon will compete directly with companies such as UPS or FedEx, offering other companies delivery services and reducing operational costs.[93] *Third*, drone delivery services can reduce traffic on the roads and carbon emissions, as the use of trucks and heavy vehicles, along with traffic congestion in cities, will drop as drone use rises.[94]

Fourth, drone delivery services are likely to increase the safety of delivery and secure product delivery. Since drones are unmanned, and the risk of drones colliding in the sky is extremely rare,[95] using them for delivery would reduce, or even eliminate, personal injury from delivery traditionally caused by motor vehicle accidents.[96] *Fifth*, the use of delivery drones could benefit the environment as using drones would reduce road traffic and the resultant air pollution.[97] Therefore, drones can be part of the solution to environmental pollution and global warming. *Sixth*, the commercial needs of drone deliveries could drive new markets and expand business and innovative development of new technology to improve drones.[98] Such

---

91 *See* Ram et al., *supra* note 87 ("[W]hile ordering any shipment, the customers can select their saved location like work or home, or they can also let the drone track the customer's location real time and deliver it on the go.").

92 *See* Ivanov, *supra* note 18, at 1501, 1510 (discussing how "over 150 guests at the OppiKoppi music festival in South Africa received cold beer via drone, giving the recipients the convenience of delivery while cutting down on the labor cost of delivery"); Margot E. Kaminski, *Regulating Real-World Surveillance*, 90 WASH. L. REV. 1113, 1120 (2015) (discussing how "[d]rones are cheaper than helicopters, easier to operate, and provide a different vantage point than cellphone cameras").

93 *See* Ram et al., *supra* note 87, at 390 ("Amazon is expected to vertically integrate by acquiring French company Colis Privé."); Enrique Dans, *The Logistics War Enters A New Phase*, FORBES (July 2, 2019), https://www.forbes.com/sites/enriquedans/2019/07/02/the-logistics-war-enters-a-newphase/?sh=688496ee228a [https://perma.cc/9WWE-6QAP].

94 Malik Doole, *Estimation of Traffic Density from Drone-Based Delivery in Very Low-Level Urban Airspace*, 88 J. AIR TRANSPORT MGMT. (2020); *see also* Ram et al., *supra* note 87, at 396 (explaining that when delivery services use drones instead of trucks there would be less trucks on the roads and the general public can get to where their want faster).

95 *See* Hwang & Choe, *supra* note 20, at 3251 (noting how "users are provided with flight information (e.g. location, altitude and route) and safety information (e.g. weather, airspace congestion and obstacles). Therefore, the risk of drones colliding in the sky is extremely rare.").

96 Hwang and Choe, *supra* note 20, at 3251.

97 Jinsoo Hwang, Woohyoung Kim & Jinkyung Jenny Kim, *Application of the Value-Belief-Norm Model to Environmentally Friendly Drone Food Delivery Services*, INT'L J. CONTEMP. HOSPITALITY MGMT. (2020).

98 Ram et al., *supra* note 87..

technological innovation could lead to progress, create jobs and bring economic prosperity.

C. The Flip Side: Invasion of Privacy

1. Drones, Surveillance Capabilities and Platform Data Analysis

Delivery drones have unique surveillance capabilities with a greater range than anything before them. These "eyes in the sky" are becoming smaller and more powerful and are able to remain in the sky longer. "They're being designed to follow you where you go."[99] The quality of surveillance measures, their omnipresence, their ability to collect and maintain personal information, and the ability of their platforms to analyze such information, draw conclusions about data subjects and even manipulate them, can result in far-reaching surveillance. The following subsections will overview the unique parameters of drone delivery surveillance:

1) The ability to reach: drones are able to observe places "from the bird's fly" and reach spaces the human eye cannot necessarily see. They are smaller than most aerial platforms, they provide a different vantage point than cellphone cameras and can reach places that other arial platforms are usually unable to observe. [100]

2) The ability to "see": the sophisticated cameras with which many delivery drones are equipped allow them to take high-resolution pictures, far beyond the capacity of the naked eye. Such cameras allow drones to acquire imagery that includes "intimate details." For example, drones could identify the topic of a news article a person is reading while sitting in his fenced backyard.[101]

3) The ability to recognize: delivery drones operate in the service of large commercial platforms such as Amazon. In some cases, the platform has a database of images of their customers and they can use facial recognition technology[102] to automatically link between the

---

99 WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 247 (2018).

100 Bennett, *supra* note 47; Kaminski, *supra* note 92, at 1120.

101 Villasenor, *supra* note 27.

102 *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 421–22 (2017) (explaining that the use of AI machine learning is becoming more prevalent. As a result, everyone in public is likely to be identified through facial recognition); Woodrow Hartzog & Evan Selinger, *Why You Can No Longer Get Lost in the Crowd*, N.Y. TIMES (Apr. 17, 2019), https://www.nytimes.com/2019/04/17/opinion/data-privacy.html [https://perma.cc/R5MK-

people captured by drone cameras and their names, allowing identification in houses or on the street.[103]

4) The ability to "hear": delivery drones can include recording systems that are capable of recording conversations from afar, way beyond the ability of the unaided ear. Such technologies could enable them to collect highly sensitive personal information that most people would prefer to keep private from the public. Using amplification to listen to conversations "prevents the subject of surveillance from adjusting her degree of disclosure appropriately because it does not provide notice to the subject the way visibly standing nearby might."[104]

5) The ability to record and the permanency of recording: technologies of recording which capture camera images create a permanent record that is qualitatively different from note-taking or memory and different than just watching or listening.[105]

6) Continuing omnipresent surveillance: commercial companies have drone fleets that never sleep, blink, get confused or lose their attention span. Together, the drones can monitor everyone automatically and composite a record of every movement by using networked cameras, sensors and recording systems. Such technologies allow drones to capture individuals continually and not only at specific moments.[106]

7) Continuing data collection, analysis and influence: platforms that sell merchandise or food, such as Amazon, operate a

---

Q3MW]; Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/N9P5-TEGC].

103 *See* Malkia Devich-Cyril, *Defund Facial Recognition*, THE ATLANTIC (July 5, 2020) https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ [https://perma.cc/MN8A-7MGV] ("In the past few weeks, Homeland Security has spied on protesters in 15 cities using drone surveillance, while police body cameras equipped with facial-recognition technology have captured images of protesters."); Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33, 101-02 (2019) ("[T]he experience of using facial recognition technology, a tool that is used for racial profiling and tracking in China and to scan the streets of Russia for 'people of interest,' can feel like a godsend, saving us and everyone else who socially conforms from waiting in long frustrating lines.").

104 Kaminski, *supra* note 92, at 1149-50.

105 Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIRCUIT 57, 61 (2013); *see also* Kaminski, *supra* note 92, at 1118 (discussing how "[d]rones—with their ability to record individuals in public, from new vantage points, and at lower cost—are one technology driving the enactment of new privacy laws").

106 *See* Kaminski, *supra* note 92, at 1120 (discussing how "[drones] also can capture information continuously, rather than at the behest of a user").

network of drone fleets that allows them to aggregate information on actual and potential consumers without their awareness. Today drones can collect information, analyze it and transfer it to the platforms in real time.[107] The platforms aggregate the information from all their drone fleets, combine it and analyze it by using new technologies such as Big Data and Artificial Intelligence. Next, the platforms translate raw data into behavioral insights and extract new and unpredictable value from it.[108] Platforms can gain insights on consumer personalities and desires, allowing immediate feedback on what consumers are doing, or plan to do and in turn, immediately target them with messages in ways that were previously impossible. In doing so, platforms can increasingly influence consumer decisions to order products, and even manipulate them for the benefits of the commercial platforms that operate delivery drones.[109] Such influences extend to third parties, beyond the direct consumers that order a delivery.[110] For example, by collecting and processing data, the platforms can personalize their influence on consumers, target messages accurately to susceptible consumers, or to potential consumers, rendering their influence effective.[111] While previous models of influence in the marketing industry were based on exploiting *general* behavioral insights, heuristics and biases, normally using the general public's bounded rationality and vulnerabilities,[112] the new data driven models, which drone technology maintains and strengthens, do not settle for the mere exploitation of collective cognitive limitations of consumers. Instead, such models exploit the unique biases of each and

---

107 John Walicki, *Program a Tello Drone to take Pictures and then Classify the Images*, IBM DEVELOPER (May 21, 2019).

108 Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 867 (2016).

109 Joseph Turow, *Americans and Marketplace Privacy: Seven Annenberg National Surveys in Perspective*, in THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 151 (2018); SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019); *See in a related context* Richards & Hartzog, *supra* note 58, at 12.

110 *See* Balkin, *supra* note 59, at 16 (discussing how "the data that companies gather from end users can have significant external effects on third parties who may not even be users of the site. As digital companies know more about a given person, they can also know more about other people who are similar to that person or are connected to that person").

111 See in a related context Alexander Tsesis, *Marketplace of Ideas, Privacy, and the Digital Audience*, 94 NOTRE DAME L. REV. 1585 (2019); ZUBOFF, *supra* note 109, at 201-02.

112 On the problem of bounded rationality, see Daniel Kahneman, *Maps of Bounded Rationality: Psychology for Behavioral Economics*, 93 AM. ECON. REV. 1449, 1449 (2003) (explaining that when individuals make decisions, their rationality is limited by systematic biases that separate the choices they make from the optimal beliefs and choices assumed in economic rational-agent models); Herbert A. Simon, *A Behavioral Model of Rational Choice*, 69 Q.J. ECON. 99 (1955).

every individual.[113] By using the knowledge gained through continuing surveillance and information collection, platforms can influence consumer decisions by using subliminal cues, designed to shape behavior at the precise time and place when maximum influence is possible, at a variety of pressure points.[114] The quality and quantity of information collection multiplies with technology, and the rise of drones in particular, allowing platforms to develop new, increasingly powerful strategies of influence, which are different than those implemented before surveillance capitalism. In sum, they increase and enhance the phenomenon of programable people. All in all, delivery drones increase the potential surveillance and datafication of consumers and third parties, and exacerbate privacy risks.

D. Delivery Drones and Invasion of Privacy

1. Invasion of Privacy on the Books

Prominent traditional theories of privacy define the right to privacy as the right to be free from intrusion and the freedom to exclude the public, as Warren and Brandeis defined "the right to be let alone,"[115] and Gavison defined privacy as a limited right of access by others to our private spaces.[116] Personal information can reach the general public and infringe upon the negative right to privacy. Closely related to the theory of the right to be let alone is the right to limited access to the self that "recognizes the individual's desire for concealment and for being apart from others."[117] It is the "right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion," while excluding others from his private realm.[118]

Another common understanding of privacy is that it "constitutes the secrecy of certain matters."[119] Thus, public disclosure of previously concealed information violates privacy. However, violation is recognized

---

113 ZUBOFF, *supra* note 109, at 279.

114 ZUBOFF, *supra* note 109, at 295-95 (explaining how to tune behavior); Lauren E. Willis, *Deception by Design*, 34 HARV. J.L. TECH. 115, 157 (2020).

115 Warren & Brandeis, *supra* note 54; DANIEL J. SOLOVE: UNDERSTANDING PRIVACY 15 (2008).

116 Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 571 (2015) referring to Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 446-47 (1980); *See also* SOLOVE, *supra* note 115 at 20-21 (discussing Gavison's views on limited-access rights).

117 Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L REV. 1087, 1102 (2002).

118 *Id.* at 1103, (quoting E.L. Godkin, *Libel and Its Legal Remedy*, 12 J. SOC. SCI. 69, 80 (1880)).

119 *Id.* at 1105.

only in cases of complete secrecy, "when concealed data is revealed to others."[120] Yet when the information is not previously hidden, or in cases where surveillance occurs in a public place "no privacy interest is implicated by the collection or dissemination of the information."[121]

Other theories focus on control over private information. Accordingly, individuals have a right to decide for themselves when, how, and to what extent information about them is communicated to others. The control-over-information theory of privacy dictates that all information over which individuals wish to retain control should be protected as private.[122] Yet, it fails to define the types of information over which individuals should retain control.[123] Moreover, "individuals can never be fully in control. To be effective, control cannot just be placed in the hands of individuals; control must come from society."[124]

Furthermore, some existing theories of privacy focus on personhood. Invasion of privacy disrespects individuality and personhood.[125] Privacy protects aspects of the self. In other words, it protects a person's individuality, dignity and autonomy. A person who knows that he is constantly being watched feels like a tool, and not a free person with sensibilities, ends and aspirations of his own.[126] Invasion of privacy infringes on dignity, personal autonomy and self-determination,[127] and can affect personal freedom.[128] This theory "focus[es] on limiting state intervention in our decisions often gives too little attention to the private sector. Merely restricting state interference is not always sufficient to protect privacy."[129] An expansion of the conception of privacy as a protection of personhood is the protection of intimacy. Accordingly, privacy should expand beyond the protection of the individual self and protect human relationships.[130] Intimate relationships need a space free from the gaze of crowds in order to allow self-disclosure

---

120 Daniel J. Solove, *A Taxonomy of Privacy,* 154 U. PA. L. REV. 477, 497 (2006).

121 *Id.*; *see also* Solove, *supra* note 117, at 1107 ("In a variety of legal contexts, the view of privacy as secrecy often leads to the conclusion that once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private").

122 Solove, *supra* note 117, at 1112 (citing ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).

123 *Id.* at 1115.

124 Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. (forthcoming 2023) (manuscript at 17).

125 *See* SOLOVE, *supra* note 115, at 30 (discussing the personhood conception of privacy); Solove, *supra* note 117, at 1116 (introducing the concept of privacy protecting personhood).

126 *See* Solove, *supra* note 117, at 1116 (discussing how privacy affects personhood).

127 ARI EZRA WALDMAN, PRIVACY AS TRUST 27 (2018).

128 *Id*. at 29.

129 Solove, *supra* note 117, at 1118.

130 *Id.* at 1121.

and development of the individual through the relationship. This theory does not define intimacy and excludes many matters that do not involve intimate relationships.[131]

The theories overviewed above reflect an understanding of the right to privacy as an individual negative right, leading to a vague understanding of the scope of the right and the types of harm a right to privacy should address. The focus of traditional conceptions of privacy is on the individual's negative right to protection from unwanted intrusion. Consequently, policy approaches are based on an individual's subjective exercise of privacy rights and the principle of reasonable expectation to privacy. These approaches allow waiver of privacy by consent.

a. Reasonable Expectation to Privacy

The "reasonable expectation to privacy" principle dictates the scope of privacy interests. This principle was developed within the context of Fourth Amendment protection against invasion of privacy by the state. Five decades ago, the Supreme Court in *Katz v. United States*[132] determined that Fourth Amendment protection applies when a person exhibits an "actual (subjective) expectation of privacy. . .that society is prepared to recognize as 'reasonable.'"[133] This test has been implemented in civil privacy torts.[134] Factors courts have weighed in determining whether a plaintiff has a reasonable expectation to privacy include: location, time of day, relationship to the observer and more.[135] However, "[w]hile individuals generally have a reasonable expectation of privacy from intrusions into their homes, there is a lesser expectation of privacy from being observed on one's property (outside the confines of the home)."[136] Moreover, the expectation of privacy

131 *Id.* at 1124.

132 389 U.S. 347 (1967) (ruling that warrantless electronic bugging in a public telephone booth are unconstitutional, thus establishing the doctrine of "legitimate expectation of privacy"); for expansion, see Andrew B. Talai, *Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age*, 102 CALIF. L. REV. 729, 753 (2014).

133 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

134 Scharf, *supra* note 52, at 1089. This article will discuss the civil privacy tort law in part II.

135 *Id.*

136 *Id.* at 1090.

is lesser in public,[137] especially when surveillance is conducted by private entities.[138]

The dichotomy of private and public has often been used by courts to determine the scope of privacy.[139] When what is viewed is "perceptible to the naked eye, or unaided ear"[140] courts have declined to recognize a reasonable expectation of privacy. Only exceptional circumstances have led courts to diverge from the presumption that there is no expectation of privacy in public.[141] Many scholars have questioned this assumption, arguing that

---

137 *See Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."). For expansion, see Waldman, *supra* note 127, at 99 (explaining that, in the United States, the law does not protect privacy regarding information that was already discovered to other people). On traditional distinction between privacy at home and privacy outside the home and criticism of such distinction in the digital age, see Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technological Change*, 70 MD. L. REV. 614, 661 (2011) (discussing the limitation of an analogous content/noncontent distinction).

138 *See* Margot E. Kaminski, *Regulating Real-World Surveillance,* 90 WASH. L. REV. 1113, 1126-27 (2015) ("Under a variety of constitutional justifications—stemming from both the Fourth Amendment and the First Amendment—it can be argued that ordinary activities performed in public should be protected from government surveillance. However, when private citizens conduct surveillance on other private citizens, the question of privacy harm becomes more complicated.").

139 *See e.g.,* Solove, *supra* note 117 at 1107 (discussing the fact that there is no reasonable expectation of privacy in things exposed to the public); *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1523 (2010) (noting the deficiencies in behavioral data asking about people's views of where they expect privacy); California v. Greenwood 486 U.S. 35 (1988) (holding that there is no reasonable expectation of privacy in garbage because it is knowingly exposed to the public); Florida v. Riley, 488 U.S. 445 (1989) (holding that the Fourth Amendment does not apply to surveillance on a person's property from an aircraft flying in navigable airspace because the surveillance was conducted from a public vantage point); Dow Chem. Co. v. United States, 476 U.S. 227 (1986) (holding that where a surveillance camera was used to observe the open areas of an industrial facility, no search occurred); California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that naked-eye observations of a fenced-in backyard deemed within the home's curtilage from an aircraft at one thousand feet did not constitute a search because, "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed . . . ."); Nussenzweig v. DiCorcia, No. 108446/05, 2006 WL 304832, at 7-8 (N.Y. Sup. Ct. Feb. 8, 2006) (holding that photographing an Orthodox Jewish person in public by a prominent photographer, unbeknownst to him, is not an invasion of privacy).

140 People v. Amo 153 Cal. Rptr. 624, 627 (1979) ("So long as that which is viewed or heard is perceptible to the naked eye or unaided ear, the person seen or heard has no reasonable expectation of privacy in what occurs."); United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

141 *See e.g.,* Kaminski*, supra* note 105 at 70 (giving some examples of cases where courts have found an expectation of privacy in public); Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964) (holding that a photograph of a woman's underwear, taken in public, was still considered an

the term "public" has never been properly defined and that the term is value laden. Thus, they have advocated a theory of privacy that focuses on enabling participation in social spaces.[142] To date however, there is generally no limitation on photographing or observing individuals in public.[143]

b. The Concept of Consent

Most theories treat privacy as an individual right, emphasizing the centrality of individual choice. Consent bolsters autonomy and choice. "When consent is present, trespassers can become dinner guests, a battery can become a welcome pat on the back, and even what would otherwise be a sexual assault can become an act of intimacy."[144] This concept declines to make a value judgement about whether certain forms of invasion, collecting, using, or disclosing personal data are good or bad. Rather, the Concept of Consent asks whether a person has agreed to the privacy practice in question. Consent to the practice, whether invasion of privacy, data collection, use or disclosure, renders the practice legitimate.[145] Consent is particularly strong in agreements between parties who have equal bargaining footing, significant resources, and "who *knowingly* and *voluntarily* agree to assume contractual or other legal obligations."[146] The idea that privacy is a concept of the autonomous self is grounded in the assumption that the liberal self-possesses a right to rational deliberation and choice.[147] However, as we will explain

invasion of privacy); Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998) (holding that a victim of a car crash can have an expectation of privacy in her conversations with a nurse and other rescuers, even though the crash took place in public).

142 *See e.g.,* Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1290–92 (2018) ("The question of what is public, however, is often just a plot on the spectrum of things that range from completely obscure to totally obvious or known."); Selinger & Hartzog, *supra* note 103, at 96 (2018) (arguing that there is no dichotomy between private and public and thus, privacy concerns degrees of obscuring); Woodrow Hartzog, *The Public Information Fallacy*, 99 B.U. L. REV. 459, 513 (2019) (arguing that there is no clear definition of public information, and the notion of public information is value-laden: "To say something is 'public' is to make a value-laden conclusion about what information should be protected and what kinds of surveillance and data practices should be permissible. It is an exercise of power.").

143 Restatement (Second) of Torts § 652B cmt. c. (Am. L. Inst. 1977) (advising that there is no general interest of privacy in public "since he is not then in seclusion, and his appearance is public and open to the public eye").

144 Neil Richards and Woodrow Hartzog, *The Pathologies of Digital Consent,* 96 WASH. UNIV. L. REV. 1461, 1462 (2019).

145 *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) ("Consent legitimizes nearly any form of collection, use, or disclosure of personal data.").

146 Richards & Hartzog, *supra* note 144, at 1463.

147 Julie E. Cohen*, What Privacy Is For*, 126 HARV. L. REV. 1904, 1907 (2013).

below, consent often falls short of this "gold standard"[148] and individual autonomy is violated.

E. When Privacy and Delivery Drones Collide: Traditional Conceptions Collapse

The unique ability of drones to easily and inexpensively record observations from above using imaging cameras and other information-gathering tools results in robust invasions of various types, which differ in quality and quantity from previously known privacy violations.[149]

Ongoing invasions of privacy by networks of drone fleets, the ability of the platforms that operate them to recognize and identify people and their private information, along with the ability to categorize individuals and draw conclusions about them[150] all have serious consequences. Invasion of privacy by drone delivery services could have a robust influence on the freedom of choice and as mentioned,[151] allow manipulation of individuals based on their personal information. Thus, drone delivery services are located at the complex intersection between technology and privacy.

Today, the conflict between technology and privacy shatters reasonable expectations of privacy, as scientific advances alter our understanding of what is possible, and therefore expected. This conflict collapses traditional distinctions between the private and public spheres, and the notion that there is no privacy in public no longer seems appropriate.[152] In other words, the interaction between technology and privacy erodes the dichotomy between

---

148 Richards & Hartzog, *supra* note 144, at 1463; *see also* Daniel J Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. (forthcoming) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743 ("[P]rivacy consent is fraught with problems. Most privacy consent is a fiction.").

149 *See* United States v. Maynard, 615 F.3d 544, 561 n.* (D.C. Cir. 2010) (explaining the idea that the "whole" can result in a different privacy consideration than the "parts"), *aff'd in part sub nom*. United States v. Jones, 132 S. Ct. 945 (2012); Andrew B. Talai *Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age,* CALIF. L. REV. 729, 757 (2014) (discussing the *Maynard* and *Jones* decisions).

150 On aggregation of data and algorithmic analysis, see FRANK PASQUALE: THE BLACK BOX SOCIETY 165 (2015).

151 *See* part I.3 (7) (referring to the ability of drones to continuing data collection, that transferred to the platform , undergo analysis and is used for influence).

152 Empirical studies discovered that the ease of accessibility of information in the public sphere does not drive judgments of appropriateness of its dissemination, and reasonable expectations of privacy can exist for public records. Therefore, assessments of privacy should be more nuanced. *See* Kirsten Martin & Helen Nissenbaum, *Privacy Interests in Public Records: An Empirical Investigation*, 31 HARV. J.L. & TECH. 111 (2017) (conducting research into privacy perception surrounding public information).

private and public.[153] It takes surveillance a step further, shifting constant collection and retention of data from opt-in to opt-out, and empties traditional concepts of consent. According to current regulation, if the invasion of privacy solely concerns the privacy of consumers of platforms operating delivery drones (as opposed to invasion of privacy of third parties) and consumers "agree" to the privacy terms (usually with little understanding of the terms of the bargain, or power to negotiate or opt out), there is no privacy violation.[154] However, when it comes to human information, the talk of "choice" is an illusion.[155] Consumers don't always understand the technology with which drones are equipped, or the privacy risks of delivery drones, and they lack the ability to assess the risks of future harm from the collection, use and disclosure of their data.[156] Moreover, in some cases, individuals have no choice but to consent, because there is no alternative to the service.[157] For example, during COVID-19 lockdowns individuals were in fact forced to agree to the terms of service of Zoom, an essential program for their work and for their children's distant learning. Such digital services became indispensable to us, in order to be full participants in society.[158] Consumers therefore click the consent button without even reading the terms of the agreement.[159]

Traditional theories that define privacy as a negative right, and protect spheres around individuals by requiring others to avoid intrusion, are ill-equipped to treat violations perpetrated by delivery drones and the

---

153 See generally Villasenor, *supra* note 27, at 459 for a discussion on the collapse of traditional privacy presumptions.

154 Kenneth A. Bamberger & Ariel Evan Mayse, *Pre-Modern Insights for Post-Modern Privacy: Jewish Law Lessons for the Big Data Age* 3-4, (Jan. 2021) (unpublished manuscript).

155 NEIL RICHARDS: WHY PRIVACY MATTERS 174 (2021); ARI EZRA WALDMAN, INDUSTRY INBOUND: THE INSIDE STORY OF PRIVACY, DATA AND CORPORATE POWER 170-171 (2021).

156 Balkin, *supra* note 59, at 16; *see also* Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 852-53 (2022) ("When people use an app that thwarts their privacy expectations, people's ability to assess the risks of using the app is impeded. The market cannot work fairly if people's expectations are completely wrong, if people lack knowledge of potential future uses of their personal data, and if people have no way to balance the benefits and risks of using products or services.").

157 Richards & Hartzog, *supra* note 144, at 1486 (referring to three pathologies of consent and defining *coerced consent* as "a choice that takes the 'voluntary' out of 'knowing and voluntary'"). For example, during COVID-19 lockdowns, one of the only options to get meals was by using Wolt for food delivery, as the restaurants were closed for T.A.

158 *See* CARISSA VELIZ: PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 39 (2020), NEIL RICHARDS: WHY PRIVACY MATTERS 54 (2021) (explaining that the choice is a fiction when we are presented with the choice of whether or not to participate in the digital world).

159 OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2014) (discussing the contours of consent).

challenges these drones pose to privacy. Such challenges concern informational privacy that covers interests in an individual's private data, its collection and dissemination, and the manner in which the data is collected, analyzed, and disclosed. Such interests extend beyond the disclosure of private lives and reach a multitude of spheres of harm. [160]

The following subsections will overview common types of invasion of privacy by drones and the harm caused by them. It will demonstrate how the dichotomy between private and public collapses and the concept of consent falls short of addressing the manner and context of information collection, processing and use.

1. Invasion of Privacy at Home

The first type of privacy concern is a direct violation of the right to privacy at home. Imagine a person is at home, when suddenly the person hears a noisy buzz, looks out the window and sees a drone hovering a few feet away peering into the window.[161] Such an invasion *violates the reasonable expectation of privacy*, as individuals have a reasonable expectation of privacy from intrusion into their homes,[162] even where there is no physical intrusion into the home.[163] Thus, when a couple in Orem, Utah used a drone

---

160 Bamberger & Mayse, *supra* note 154, at 15 (explaining that privacy had been defined in theory mostly as a "negative liberty," and noting as a result, policy discussions focus on protecting the privacy of individuals rather than curtailing the surveillance activities of organizations) (citing PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY, at 3 (1995)).

161 *See* Rebecca J. Rosen, *So This is How it Begins: Guy Refuses to Stop Drone-Spying on Seattle Woman*, THE ATLANTIC (May 13, 2013), http://www.theatlantic.com/technology/archive/2013/05/so-this-is-how-it-begins-guy-refuses-to-stop-drone-spying-on-seattle-woman/275769/ [https://perma.cc/8FHG-UXNG] (describing a complaint about a drone flying feet away from a woman's window).

162 Scharf, *supra* note 52, at 1090; *see also* Strandburg, *supra* note 137, at 618 (describing the entrance to the home as the "bastion of Fourth Amendment privacy"); Bamberger & Mayse, *supra* note 154, at 55 ("The fragmented nature of privacy protections—focusing on specific places (the 'home'), or types of data—fail to appreciate the totality of big-data surveillance . . . .").

163 In the past, physical intrusion was part of the concept of invasion under the Fourth Amendment. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 466 (1928) (explaining that one historical violation of the Fourth Amendment was an "actual physical invasion"). But this formulation has changed because technology can also invade a person's privacy when it invades a person's home. *See* Kyllo v. United States, 533 U.S. 27, 29-30, 40 (2001) (holding that the police investigation using a thermal imager—i.e., a sense-enhancing technology that was not publicly available at the time—to collect any information regarding interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a "search"); *see also* Talai, *supra* note 132, at 764 ("To summarize, the reasonable expectation of privacy test . . . may provide some protection for certain details of the home discovered by generally unavailable technology.").

equipped with a video camera to observe neighbors in their homes, and the drone was spotted outside the bathroom of one of the victims, they were charged with a misdemeanor of voyeurism using concealed or disguised electronic equipment.[164]

Although drones are unmanned and there is no human eye looking into the person's home in real time, the operator can see the pictures the drone takes and even duplicate them.[165] Moreover, with the advancement of technology drones can transmit the pictures or videos they take to their operators in real time. Thus, when a drone peers directly into a home it violates the reasonable expectation of privacy according to traditional theories of the "negative right to privacy", as it invades private life per-se.[166]

When a person orders a delivery from a platform that operates a drone delivery service, it might be argued that the person *consents* to terms of service allowing drones to peer into windows and take pictures. Thus, even if such intrusion into the home is within the reasonable expectation of privacy, the consumer has consented to it. The concept of consent has been criticized in scholarship. It can be argued that in the digital technological context, such consent not only falls short of the gold standard, it is even flawed and should not be considered valid. Such consent may not be informed consent; it may even be coerced.[167] Consumers are busy and distracted and the privacy policy and terms of service are confusing,[168] so they just click "I agree."[169] Reading terms of service and privacy policies takes time,[170] attention is

---

164 *See* Scharf, *supra* note 52, at 1068 (describing this incident); Mary Papenfuss, *Utah Couple Arrested Over 'Peeping Tom' Drone*, HUFFINGTON POST (Feb. 17, 2017, 2:51 AM), bit.ly/38JSgwz [https://perma.cc/J9GU-2XVJ] (describing this incident).

165 *See* Villasenor, *supra* note 27, at 477 (noting how pictures taken by a camera on an airplane can be readily duplicated).

166 *See* Iwona Florek et al.,*The Need for Protection of Human Rights in Cyberspacy,* J. MOD. SCI. 3, 32 (2019) ("The negative right to privacy entails that individuals are protected from unwanted intrusion by both the state and private actors into their private life.").

167 *See* HARTZOG, *supra* note 99, at 21-54 (noting how consent to privacy settings does not match with users' intentions); *see also* Richards & Hartzog, *supra* note 144, at 1478 (referring to types of consent that are not meaningful: unwitting consent, coerced consent, and incapacitated consent); *see generally* BEN-SHAHAR & SCHNEIDER, *supra* note **Error! Bookmark not defined.** (discussing the contours of consent).

168 *See generally* Benjamin Scheibehenne, Rainer Greifeneder, & Peter M. Todd, *Can There Ever Be Too Many Options? A Meta-Analytic Review of Choice Overload*, 37 J. CONSUMER RSCH. 409-21 (2010) (reviewing literature on choice overload).

169 Richards & Hartzog, *supra* note 144, at 1479.

170 *See* Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, THE ATLANTIC, (Mar. 1, 2012) (emphasizing how long it would take to read every privacy policy on websites the average American internet user visits in a year); NEIL RICHARDS: WHY PRIVACY

limited, and even when consumers do read, they may find it difficult to understand the language and assess the risk.[171] Moreover, an online platform's design can be abusive; they can nudge to their preferred direction,[172] or manipulate consent, and can even encourage unwitting consent by falsely signaling to consumers that the platform is trustworthy, thereby weakening the users resistance to information sharing.[173] For example, designers can program the platform so the default is agreeing to a drone peering into the home and collecting information, making it difficult to find the opt out option. Thus, the concept of consent provides only an illusory procedural safeguard. [174]

In summary, delivery drones that peer into homes violate the right to privacy and infringe on the negative right to privacy. Such an invasion can result in psychological distress and affect well-being.

2. Looking from Afar

The second type of invasion is "looking from afar." A drone can "look" and observe individuals in their private property without peering directly, and without trespassing or interfering with the use of property. Equipped with sophisticated, high-resolution cameras and recording systems, drones

---

MATTERS 92-108 (2021) (explaining that the concept of "privacy as control" and of consent that allows control is overwhelming, illusionary, insufficient and in fact a trap); *see also* ARI EZRA WALDMAN, INDUSTRY INBOUND: THE INSIDE STORY OF PRIVACY, DATA AND CORPORATE POWER 52 (2021) (explaining that the information industry has a strong interest in privacy as control, as it allows the industry to argue that sharing information was a choice of the user, while users actually cannot adequately process corporate privacy notices; our decision making is irrational and such consent is not the same as making a real choice).

171 *See* Daniel J. Solove, *The Myth of the Privacy Paradox*, GW L. FAC. PUBL'NS & OTHER WORKS, 35 (Feb. 11, 2020) ("In many cases, it isn't possible for people to assess privacy risks in a meaningful way."); CASS R. SUNSTEIN, TOO MUCH INFORMATION: UNDERSTANDING WHAT YOU DON'T WANT TO KNOW 85 (2020) ("[O]ne cannot help but be struck by the impossibility that anyone could attend to even a fraction of the disclosures to which we are exposed.").

172 CASS R. SUNSTEIN & RICHARD H. THALER, NUDGE: THE FINAL EDITION: IMPROVING DECISSIONS ABOUT MONEY, HEALTH, AND THE ENVIRONMENT (2021).

173 *See* Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox"*, CURRENT ISSUES IN PSYCH. 105 (2020) ("[N]otice-and-consent is ill-equipped to inform users of corporate data use practices."); *see also* Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 J. LEGAL ANALYSIS 43, 104 ("[T]he data presented here give the strongest hint yet of how large the mismatch is between what consumers want and what they are supposedly consenting to."); *see also* Willis, *supra* note 114, 170 n.245 (noting a federal law that would prohibit large companies from designing their platform in such a way to impair a user's freedom of consent); *see generally* RICHARDS: WHY PRIVACY MATTERS, at 95.

174 *See* Bamberger & Mayse, *supra* note 154, at 4 (explaining that individuals "'agree' to privacy terms, often with little understanding of the terms of the bargain . . . or power to negotiate or opt out.").

can "see" what everyone does,[175] or "hear" and record private conversations.[176] Taking pictures and recording creates a permanent record and allows the collection of highly sensitive information. Is there a *reasonable expectation of privacy*? Arguably, in an age where private commercial drones in the public airspace are a matter of routine, it is unreasonable to expect privacy when the drone looks from afar, without trespassing on private property. Observations from a public navigable airspace are not intrusions which violate a reasonable expectation of privacy.[177]

However, it can be argued that lack of reasonable expectation should be limited to that which can be viewed or heard by the naked eye or unaided ear. The reasonable expectation of privacy should not apply "to that which cannot be seen by the naked eye or heard by the unaided ear."[178]

It might be argued that when an individual orders a delivery from a platform that operates a drone delivery service, the person *consents* to the use of surveillance technology that surpasses the capacity of the human eye or ear. Yet, like consent to invasion of privacy at home, we assume that "looking from afar" with sophisticated technology can also "see" or "hear" what happens on the premises of third parties in the background, such as neighbors that did not consent to surveillance, as they did not order the delivery and are incidentally affected by the use of such drones. Moreover, as explained, consumer consent can be flawed, uninformed, and invalid.[179]

---

175 *See* Villasenor, *supra* note 27, at 464 (noting that drones equipped with "high-resolution, low-cost digital imaging systems" can send videos and images in real time).

176 Even though at this time consumer drones usually do not possess the capability to record conversations because of the noise level, with the right equipment, recording private conversation can be possible. *See Can Drones Hear Our Conversations?*, REMOTEFLYER, https://www.remoteflyer.com/can-drones-hear-our-conversations/ [https://perma.cc/2V9G- ATR7].

177 *See* California v. Ciraolo, 476 U.S. 207, 215 (1986) (holding that naked-eye observations of a fenced-in backyard deemed within the home's curtilage from an aircraft at one thousand feet did not constitute a search because, "[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."); *see also* State v. Davis, 360 P.3d 1161, 1169 (N.M. 2015) (explaining there is no reasonable expectation of privacy from aerial surveillance of the defendant's greenhouse); Jennifer A. Brobst, *Enhanced Civil Rights in Home Rule Jurisdictions: Newly Emerging UAS/Drone Use Ordinances*, 122 W. VA. L. REV. 741, 769 (2020) ("[O]bservations from public navigable airspace are not intrusions into a reasonable expectation of privacy.").

178 Lawrence Kaiser Marks, *Telescopes Binoculars and the Fourth Amendment*, 67 CORNELL L. REV. 379, 387 (1982) (citing People v. Amo, 153 Cal. Rptr. 624, 627 (Cal. Ct. App. 1979)).

179 *See* HARTZOG, *supra* note 99, at 21-54 (explaining how consent to privacy settings does not match with users' intentions); *see also* Richards & Hartzog, *supra* note 144, at 1478 (referring to types of consent that are not meaningful: unwitting consent, coerced consent and incapacitated consent); *see generally* BEN-SHAHAR & SCHNEIDER, *supra* note 159 (discussing the contours of consent).

Delivery drones can "look from afar" and observe the property of consumers and third parties without trespass.[180] In such cases, convention dictates that there should be a lesser expectation of privacy than in cases where a person peers directly into the home. However, the reasonable expectation of privacy might exist when the drone uses sophisticated technology that allows it to "see" or "hear" beyond the ability of a human eye or ear.[181] In such cases, delivery drone surveillance would infringe on consumer privacy.

The differentiation between surveillance with the naked eye or ear, and surveillance empowered by sophisticated technology considers the context in which surveillance power is amassed and used.[182] However, such consideration falls short, as it does not take into account the ability to document and record what is seen by the human eye and the context of time. Pictures and recordings taken from afar of a consumer's premises can be remembered by corporations over time. In other words, corporations can keep record of consumers' private property.[183] The absence of legal protection from permanent recordings can result in self-chill on behavior outside the house.[184] Moreover, it neglects to address the second layer of data collection and analysis, which this Article will address below in Part V.D.

3. Delivery Drone Surveillance in Public

The third type of privacy concern is surveillance in public. Drones can observe individuals in the public sphere, as they walk down public streets or in parks, travel or drive on public roads. This is true whether they are consumers or third parties. In such cases, drones do not peer directly into houses or look from afar. Both the object of the surveillance and the

---

180 See in a related context, Sean Murphy, *Animal Liberation Activists Launch Spy Drone to Test Free-Range Claims*, ABC NEWS (Aug. 30, 2013), https://www.abc.net.au/news/2013-08-30/drone-used-to-record-intensive-farm-production/4921814 [https://perma.cc/T5K2-29F8] ("So the key to the remote-controlled device is that it's actually vision that's obtained without trespass.").

181 People v. Amo, 153 Cal. Rptr. 624, 627 (Cal. Ct. App. 1979) ("So long as that which is viewed or heard is perceptible to the naked eye or unaided ear, the person seen or heard has no reasonable expectation of privacy in what occurs.").

182 *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010) on contextual integrity of information flows.

183 On the importance of forgetting for enhancing privacy and the E.U. "right to be forgotten," see Michal Lavi, *The Good, The Bad, and the Ugly Behavio*r, 40 CARDOZO L. REV. 2597, 2627, 2629-30 (2019).

184 *See* Kaminski, *supra* note 92, at 1155-56 (failing to limit permanent recordings will make people regulate the content of their conversations outside the house).

surveillance itself take place in public. In such cases, as explained,[185] the traditional interpretation of privacy theory is that there is no *reasonable expectation of privacy* in public as long as what is viewed is perceptible to the naked eye or unaided ear.[186] Courts have been willing to divert from the presumption of lack of privacy in public only under special circumstances and that contextualized understanding often relies on the inherent sensitivity of the type of information at issue, for example information related to a naked body, or taking a picture of a woman's underwear exactly when her skirt flies up.[187] In such cases, the fact that the picture was taken in the public sphere does not render it non-private.[188] Generally, there is no reasonable expectation of privacy in public, as the person's appearance is public and visible to all.[189] Therefore, there is no need for *consent*, and the relevant act would not be considered a violation of the right to privacy.

In the digital era, the general dichotomy between the private and public spheres collapses and the justification for such a distinction diminishes. The narrative that the act must involve private property in order to establish a violation is incomplete and does not account for technologies that can hinder the anonymity and obscurity of individuals in the crowd.[190] As the use of artificial intelligence (AI) becomes more prevalent, anyone in public can be tracked in the streets and identified through facial recognition technology.[191]

---

185 See Part I. D., 1. A (titled "reasonable expectation to privacy"); *see also* Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIR. 57, 70 (May 2013).

186 People v. Amo, 153 Cal. Rptr. 624, 627 (Cal. Ct. App. 1979) ("So long as that which is viewed or heard is perceptible to the naked eye or unaided ear, the person seen or heard has no reasonable expectation of privacy in what occurs."); United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); United States v. Farias-Gonzalez, 556 F.3d 1181, 1188 (11th Cir. 2009); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 495–96 (2006) ("The law often recognizes surveillance as a harm in private places but rarely in public places.").

187 *See* Daily Times Democrat v. Graham, 162 So. 2d 474, 476-77 (Ala. 1964) (ruling that publication of photographs taken in public of a woman's underwear violated her right to privacy).

188 *See* Kaminski, *supra* note 92, at 1124 ("[B]eing in a public space does not necessarily make the information non-private in nature.").

189 *See* Restatement (Second) of Torts § 652B, cmt. C (Am. L. Inst. 1977) ("Nor is there liability for . . . taking his photograph while he is walking on the public highway . . . [because] his appearance is public and open to the public eye."); *See, e.g.*, Nussenzweig v. DiCorcia, No. 108446/05, 2006 WL 304832, at *3, 8 (N.Y. Sup. Ct. Feb. 8, 2006) (photographing an Orthodox Jewish in public by a prominent photographer, unbeknownst to him, is not an invasion of privacy).

190 *See* HARTZOG, *supra* note 99, at 248 (describing how the narrative of Peeping Tom does not account for facial recognition technologies).

191 *See* Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 U.C. DAVIS L. REV. 399, 420–21 (2017) (noting this ability and highlighting how it threatens to "eviscerate the already unstable boundary between what is public and what is private.").

In fact, recently police forces have been known to use AI and facial recognition. There are growing concerns that it may lead to false arrests and unfair treatment of African-Americans.[192] In the context of delivery drones, surveillance can focus on specific individuals such as consumers, past consumers, or future consumers and use the information gathered by the drones in order to profile them.[193] Similar to information that is gained by looking from afar the information gained from the public sphere is not just seen and forgotten. The pictures and recordings of identified individuals in public can be "remembered" and retained by the platforms over long periods of time.[194]

Empirical studies have revealed that the public has an expectation of privacy in the public sphere.[195] Scholars have criticized the assumption that there is no privacy in public as there is no dichotomy between private and public.[196] Moreover, there is no clear definition of "public." As a result, to say that surveillance is "in public" is a conclusion about what should be permissible and an exertion of power.[197] Furthermore, as the next subsections demonstrate, data collected in the public sphere can be aggregated and used to influence consumers. However, despite the collapse

192 Amazon has lately put a one-year moratorium on police use of its facial recognition tool in hope that Congress will put stronger regulation to govern the ethical use of such technologies. *See We are Implementing a One-Year Moratorium on Police Use of Rekognition*, AMAZON (June 10, 2020), https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition [https://perma.cc/SR85-VELR].

193 *See* Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOYOLA L. REV. 33, 34 (2019) ("[F]acial recognition technology, a tool that is used for racial profiling and tracking in China and to scan the streets of Russia for 'people of interest,' can feel like a godsend, saving us and everyone else who socially conforms from waiting in long frustrating lines. The more familiar and beneficial a surveillance technology like facial recognition seems, the easier it is for technology companies, government agencies, and entrepreneurs to create conditions for widespread passive acceptance.").

194 On the importance of forgetting for enhancing privacy and the E.U "right to be forgotten," see Lavi, *supra* note 183, at 2627, 2629-30.

195 *See* Martin & Nissenbaum, *supra* note 152, at 117 (arguing that the ease of accessibility of information in the public sphere does not drive judgments of appropriateness of its dissemination, and reasonable expectations of privacy can exist for public records).

196 *See, e.g.* Martin & Nissenbaum, *supra* note 152, at 112–13.; Hartzog, *supra* note 129, at 513; Woodrow Hartzog, *Body Cameras and the Path to Redeem Privacy Law*, 96 N.C. L. REV. 1257, 1290–92 (2018) (arguing that there is no dichotomy between private and public. Instead, there is a spectrum that ranges from completely obscure to totally obvious or known); HARTZOG, *supra* note99, at 96.

197 Hartzog, *supra* note 142, at 513.

of the dichotomy between private and public in the face of intrusive technologies, the conception that there is no privacy in public remains.[198]

4. Data Collection, Aggregation, Analysis and Manipulation

The fourth type of privacy concern is data collection, aggregation, analysis and manipulation. The Peeping Tom narrative of drones peering into private property described above in part I. 5.A is incomplete,[199] as it focuses on negative privacy and does not take into account information privacy concerns,[200] namely "the degree to which human information is neither known or used."[201] This type of infringement of information privacy can occur in public and even without using sophisticated technology at the first stage of data collection. Privacy concerns arise when drones collect information a person does not think will be collected, the person cannot hide from such collection, and the person cannot anticipate the consequences of processing the information. For example, a drone operator collects information on the surroundings of the house and the general consumption habits of the consumer when he buys from shops and restaurants in the street. This type of consumer data can be collected and amalgamated on a massive scale.[202] In addition, a drone can collect and aggregate information on a consumer's previous orders. Platforms that operate drones can collect information on one person and use it to draw conclusions concerning third parties, as everyone's privacy depends on what others do. In fact, there is no way of living in the world without putting oneself at risk that others may make use of one's private information.[203] Such information does not necessarily

198 Bamberger & Mayse, *supra* note 154, at 55 ("Large swaths of what is dear to individuals is deemed not protected, because it can be tracked down 'in public.'"). Jonathan Olivito, *Beyond the Fourth Amendment: Limiting Drone Surveillance through the Constitutional Right to Informational Privacy*, 74 OHIO ST. L.J. 669, 702 (2013).

199 HARTZOG, *supra* note 99, at 247. For expansion on "Peeping Tom," see Jane Dunagin, *Incoming: Regulating Drones in Oklahoma*, 69 OKLA. L. REV. 457, 473–74 (2017).

200 Margot Kaminsky, *Enough With the "Sunbathing Teenager" Gambit*. SLATE: FUTURE TENSE (May 17, 2016, 9:00 AM), https://slate.com/technology/2016/05/drone-privacy-is-about-much-more-than-sunbathing-teenage-daughters.html [https://perma.cc/HP84-X42P].

201 NEIL RICHARDS: WHY PRIVACY MATTERS 22 (2021).

202 *See* JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY AND DEFINE YOUR POWER 123 (2017) (describing a company that installed cameras with 3D sensors in stores to track shopper activity in proximity to goods made by the company's client. Drone surveillance can do the same).

203 *See* Solon Barocas & Karen Levy, *Privacy Dependencies,* 95 WASH. L REV. 555 (2020) (arguing that a person's privacy depends on others' behavior).

remain in the platform owner's hands, and can be transferred to third parties.[204]

After collecting data, the platform owner can analyze it and translate it into behavioral insights about users and third parties, using new technologies that are tools for engineering humanity.[205] Big data is part of the effort as ubiquitous data collection from a variety of sources takes the data out of its original context and allows for interconnecting, analyzing, identifying and extracting new and unpredictable value from the data.[206] Complex AI algorithms mine the information from connected devices, analyze it, find connections and correlations between data items, draw conclusions about individuals and even predict their future behavior.[207] The more data platforms collect, the more accurate intimate profiles they can create[208] and the better able their predictive algorithms become in influencing end users.

Finally, the platform "operates through the means of behavioral modification."[209] Data is power: when companies have access to private information, they may influence the actions of the entity that produced it, and even third parties.[210] By collecting and processing data, platforms can personalize their influence on consumers, target messages accurately to susceptible audiences to make their influence more effective,[211] and turn consumers and third parties into tools to advance their market through digital advertising.[212] New marketing techniques differ from traditional

---

204 *See, e.g.*, Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019), on.wsj.com/2HsnY40.

205 *See* ZUBOFF, *supra* note 50 ("Surveillance capitalism unilaterally claims human experience as free raw material for translation into behavioral data."); CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY (2016).

206 Max N. Helveston, *Consumer Protection in the Age of Big Data*, 93 WASH. U. L. REV. 859, 867 (2016); Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data, 3* INT'L DATA PRIV. L. 67, 69 (2013).

207 *See* YUVAL NOAH HARARI, 21 LESSONS FOR THE 21ST CENTURY 21–22 (2018) (explaining that AI possesses two particular non-human abilities: connectivity and updatability).

208 HARTZOG, *supra* note 99, at 248.

209 ZUBOFF, *supra* note 50.

210 CARISSA VELIZ, PRIVACY IS POWER: WHY AND HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 77 (2020) ("Through manipulation of information you can. . . distort their realities until they cannot tell what is true anymore.")

211 *See* Alexander Tsesis, *supra* note 111, at 1585; Willis, *supra* note 114, at 157 ("When profitable to do so, algorithmic marketing will aim specific materials at the most vulnerable consumers at their most susceptible moments, not average consumers when they are at their most reasonable.").

212 Jack Balkin, Keynote Address, Association for Computing Machinery Symposium on Computer Science and Law: *How to Regulate (and Not Regulate) Social Media* (Oct. 28, 2019) in 1 J. FREE SPEECH & L. 72; *see also* Uta Kohl, *The Pixelated Person – Humanity in the Grip of Algorithmic Personalization*, DATA-

ones,[213] since these techniques shift from general behavioral insights to a personalized approach, offering the ability to target people's vulnerability accurately at the right place and time.[214] As technology advances, it becomes easier to manipulate consumers' deepest emotions and desires, and it becomes increasingly dangerous for individuals to simply follow their hearts.[215]

Traditional marketing models that used behavioral insights were based on the general public's bounded rationality and vulnerabilities.[216] For example, companies endeavor to predict an individual's behavior, influence the context, and nudge their consumers in transparent or non-transparent ways.[217] While previous models of influence were based on exploiting *general* insights, heuristics and biases, the new data driven models aim to exploit the unique biases of every *specific* consumer, provide the consumer with personalized experiences and deliver the most relevant content to the target,[218] shaping consumer desires.[219]

Based on the information collected by drones, the platforms that operate them may choose which consumers to approach and offer their services.[220]

DRIVEN PERSONALIZATION IN MARKETS, POLS. & L., (forthcoming) (describing the phenomenon of "algorithmic prediction of human preferences, responses and likely behaviors in numerous social domains and subsequent 'implementation' – ranging from personalised advertising and political microtargeting to precision medicine, personalised pricing and predictive policing and sentencing").

213 *See* Julie E. Cohen, *The Emergent Limbic Media System,* in LIFE AND THE LAW IN THE ERA OF DATA-DRIVEN AGENCY 60, 61 (Hildebrandt & O'Hara ed., Elgar, 2020).

214 Michal Lavi, *Targeting Exceptions*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 65, 92 (2021); Michal Lavi, *Manipulating, Lying, and Engineering the Future*, 33 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 221, 272 (2023); *See generally* ZUBOFF, *supra* note 50, at 20.

215 HARARI, *supra* note 207, at 267–68.

216 On the problem of bounded rationality, see Daniel Kahneman, *Maps of Bounded Rationality: Psychology for Behavioral Economics,* 93 AM. ECON. REV. 1449, 1449 (2003) (explaining that when individuals make decisions, their rationality is limited by systematic biases that separate the choices they make from the optimal beliefs and choices assumed in economic rational-agent models).

217 RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 6 (2008). A nudge is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives." For example, since people tend to stick with the status quo when using default options, companies try to set default rules, and thereby influence users' behavior in their preferred ways. *See id.* at 8.

218 ZUBOFF, *supra* note 50, at 279.

219 *See* Calo, *supra* note 102, at 423 ("[F]irms can manipulate other market participants through a fine-tuned understanding of the *individual* and collective cognitive limitations of consumers") (emphasis added); Ryan Calo, *Digital Market Manipulation*, 82 U. OF WASH. L. REV. 995, 1007–09 (2014).

220 Calo, *supra* note 219, at 1004. On intermediaries and other stakeholders influences on consumers by collecting information using technologies, see JOSEPH TUROW, THE AISLES HAVE EYES: HOW RETAILERS TRACK YOUR SHOPPING, STRIP YOUR PRIVACY, AND DEFINE YOUR POWER 18–19 (2017).

They can target consumers with commercial messages based on their lifestyle and patterns of location, their personality traits, current mode or emotional state, and even social relations. Visiting a psychologist's clinic? The platform that operates delivery drones might be tracking and targeting you.[221] This data allows companies that operate delivery drones to track their targets while they are offline and offer them products when they are most susceptible.[222]

Such personalized targeting can sometimes benefit consumers (if for example it nudges them to purchase healthier food, thereby improving their health),[223] but it can also be used for data opportunism and be used against consumer self-interests.[224] It can, for example, be used to push consumers to order junk food when they are most susceptible: for example, when the data collected on the consumer shows that he had a bad day and might want to comfort himself with food. Moreover, when targeting lacks transparency and does not *sufficiently* engage with consumers' *capacity for reflection and deliberation,*[225] it infringes on consumers' autonomy to make informed decisions, hindering autonomy to mindfully choose between options.[226] Furthermore, such influence can generate suboptimal transactions, because the platform that operates drones can target consumers against their long-term preferences, leading to waste and inefficiency.[227]

New data contexts do not fall into traditional privacy theories and reasonable *expectations of privacy* are often not recognized,[228] even though consumers usually do not expect their private information to be used in such

---

221 See in a related context, *Your Mental Health for Sale,* PRIV. INT'L, bit.ly/2lK6Gag [https://perma.cc/G7X8-ZH65].

222 See e.g., in a related context, TUROW, *supra* note 202, at 127 (referring to "inMarket" a commercial company that made deals with many retailers to place Bluetooth Low Energy (BLE) boxes with the inMarket code throughout their stores. This included the right to put inMarket codes in those retailers' apps, so when shoppers placed the apps on their phones, they could be pinged by the inMarket boxes as they moved through the stores).

223 Sarah Bates et al., *A Narrative Review of Online Food Delivery in Australia: Challenges and Opportunities for Public Health Nutrition Policy*, PUB. HEALTH NUTRITION (2019), at 8.

224 Richards & Hartzog, *supra* note 58, at 12 (referring to profiling and sorting, nudges and manipulation).

225 CASS SUNSTEIN: THE ETHICS OF INFLUENCE – GOVERNMENT IN THE AGE OF BEHAVIORAL SCIENCE 82 (2016).

226 *See* Bamberger & Mayse, *supra* note 154, at 62 ("Aggregation of data facilitates the construction of narratives that manipulate one's behavior, and diminish the essence of humanity: individual choice and personal growth."); Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEORETICAL INQ. *L.* 157, 174 (2019).

227 *See* Calo, *supra* note 219, at 1025 (describing how digital market manipulation leads to consumption of "junk food" and thus preferring short time preferences over long term preferences).

228 Bamberger & Mayse, *supra* note 154, at 8.

ways and their expectations regarding the flow of information are not met.[229] Therefore, one can argue that there is no need for *consent* to such invasion of privacy. Furthermore, even if there is a recognized expectation of privacy, it can be argued that consumers consent to the use of their data when they use a drone delivery platform and "agree" to the terms of service, even though such consent is based on shaky ground.[230]

In summary, the conception of a drone invasion of privacy focuses on privacy as a negative right and on the narrative of a Peeping Tom that shapes case law. Large parts of "what is dear and personal to individuals is deemed unprotected because it can be tracked down in public . . . or because it is not reasonable to expect it to remain private in the face of intrusive technological capacity."[231] Drones identify individuals in public and collect information on "where an individual goes on a daily basis"[232] and who the individual interacts with. Drones can transmit the information to the platform, which can aggregate it and subject it to Big Data analysis, milking additional information from the data.[233] The platform can in turn use the information to influence consumer decision making without transparency. The traditional conception of privacy intrusion fails to address massive data collection and aggregation and is ill-equipped to address drone delivery violations of privacy.

The following part will overview common law regulation applicable to drone delivery services. It will argue that current U.S. law is shorthanded and neglects to remedy the harm of different types of privacy violations. It will then argue that a new framework should be set forth to recognize the need for privacy rights even during the collection, transmission and processing of the information, and even if the information was collected in "public".

II. DRONE DELIVERY AND THE LAW

There is no federal omnibus privacy law in the U.S., federal privacy law includes a series of sectoral regulations. Drone-specific regulation adds to

229 *See* NISSENBAUM, *supra* note 182, at 231.

230 *See supra* note 169 and the text attached to it; Richards & Hartzog, *supra* note 144, at 1479.

231 Bamberger & Mayse, *supra* note 154, at 55.

232 Jeramie D. Scott, *Drone Surveillance: The FAA's Obligation to Respond to the Privacy Risks*, 44 FORDHAM URB. L.J. 767, 775, 778 (2017).

233 *Id.* at 778.

this patchwork.[234] As mentioned above, the most classic instance of invasion of privacy rights is a "Peeping Tom": taking a camera-equipped drone into town and hovering it near a bedroom window.[235] This would constitute a criminal offense, since there is a prohibition against peeking into private homes under certain circumstances.[236] The application of criminal law in this context is narrow, as it focuses exclusively on an intentional act of peering into a person's house, with intent to gaze at a person or view private areas of the body, and the "Peeping Tom" must be caught in action.[237] Thus, the application of these laws to commercial drones would be rare. In the following part, this Article will address broader legislation that could remedy drone related violations of privacy in a wider range of circumstances, although this broader legislation would not cover all types of drone related violations of privacy.

A. Civil Law: Privacy Torts

In 1960, Professor William Prosser published a seminal article on common law privacy torts. The Article sought to categorize 300 appellate court cases into four distinct torts, each describing invasion of a different privacy interest and representing different interferences with the right to be let alone.[238] The categories were later codified into torts in the Restatement (Second) of Torts, with the objective of protecting personal privacy.[239] These torts have hence been referred to as "the right to be let alone". The four torts are: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) false light and (4) appropriation.[240] The tort that is most relevant with respect

---

234 *See* Kaminski, *supra* note 105, at 65 ("One federal statute governs privacy in video watching, one governs drivers' license information, one governs health information, one governs financial privacy, and so on.").

235 Colleen Wright, *Regulatory Vacuum Exposed After "Peeping Drone" Incident*, SEATTLE TIMES (July 7, 2014, 12:44 PM), bit.ly/3h4fTCM [https://perma.cc/PK9G-L5MH].

236 *See* Kaminski, *supra* note 92, at 1144 (citing GA. CODE ANN. § 16-11-61(b) (West, Westlaw through 2015 Reg. Sess.)) (defining "peeping Tom" as one "who peeps through windows or doors, or other like places . . . for the purpose of spying upon or invading the privacy of the persons spied upon and the doing of any other acts of a similar nature which invade the privacy of such persons").

237 Kaminski, *supra* note 105, at 68; Jane Dunagin, *Incoming: Regulating Drones in Oklahoma*, 69 OKLA L. REV. 457, 473 (2017); *see, e.g.*, 21 OKLA. STAT. § 1171(A) (2011).

238 William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960) (identifying the four generalized torts to be intrusion upon solitude, public disclosure of embarrassing information, public characterization of an individual in a false light, and appropriation of an individual's name or likeness); Scharf, *supra* note 52, at 1086.

239 *See generally* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010).

240 Restatement (Second) of Torts §§ 652A-652E (Am. L. Inst. 1977); Scharf, *supra* note 52, at 1086.

to delivery drones is intrusion upon seclusion.[241] Individuals who feel that a drone has violated their "right to be let alone" can file an action against the operator for intrusion upon seclusion, as this tort does not require a physical intrusion to be actionable.[242] Sometimes, the emphasis is on whether the information is private, and sometimes the emphasis is on how the information is obtained.[243] Intrusion into a plaintiff's "solitude or seclusion" happens when "[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."[244] The plaintiff must establish a subjective and objective reasonable expectation of privacy.[245] Surveillance of an individual's home would constitute an intrusion upon seclusion.[246] Courts are divided on whether the mere installation of recording technology in inherently private places constitutes an intrusion.[247]

Individuals generally have a reasonable expectation of privacy from intrusion into their homes, but there is a lesser expectation of privacy outside home, even though some courts have recognized that an expectation of privacy can exist in public regarding "looking from afar."[248] Thus, claims regarding invasions of privacy by delivery drones based on civil torts are likely to succeed when the drone peers into a home. They might also succeed in some courts regarding "looking from afar." Yet, a successful intrusion upon seclusion claim is less likely to succeed when the intrusion occurs in

---

241 Villasenor, *supra* note 27, at 501, 503. It should be noted that public disclosure of private facts might be relevant to drones in general, but delivery drones are not likely to publicize the pictures they take to the general public. The main problems are the invasion itself and the collection of information.

242 *See* Restatement (second) of Torts § 652B cmt. b (Am. L. Inst. 1977), Scharf, *supra* note 52, at 1086.

243 Kaminski, *supra* note 105, at 65.

244 Restatement (Second) of Torts § 652B; Scharf, *supra* note 52, at 1087.

245 Scharf, *supra* note 52, at 1089.

246 *Id.*; *see, e.g.*, Wolfson v. Lewis, 924 F. Supp. 1413, 1417–18 (E.D. Pa. 1996).

247 *See* Scharf, *supra* note 52, at 1089 ("Courts, however, are divided on whether the mere installation of recording technology in inherently private places constitutes an intrusion. Some courts have held that, in inherently private places -one's bedroom or the restroom-plaintiffs need not prove that a tortfeasor using technology to intrude actually listened or watched personally for an actionable claim.")

248 Scharf, *supra* note 52, at 1091; *see also* Huskey v. Nat'l. Broad. Co., 632 F. Supp. 1282, 1287 (N.D. Ill. 1986) (discussing a claim of a prisoner against a news organization which survived a motion to dismiss as the court noted that "[o]f course [the prisoner] *could* be seen by guards, prison personnel and inmates, and obviously he was in fact seen by [the defendant's] camera operator. But the mere fact a person can be seen by others does not mean that person cannot legally be 'secluded.'"); *but see* McClain v. Boise Cascade Corp, 533 P.2d 343, 346 (Or. 1975) (holding that individuals can be recorded without their knowledge or consent when those individuals are conducting themselves in public view and the recording is conducted unobtrusively).

public and it is difficult to substantiate a reasonable expectation of privacy in public spaces.[249] Such a claim would only succeed in rare situations, such as publication of a photograph of a woman with her skirt flying up taken in a public place,[250] or filming and recording for a television program at the scene of an accident without consent from the people involved.[251]

As privacy torts are less likely to succeed regarding invasions of privacy in public, they are also ill-equipped to address privacy concerns regarding delivery drone data collection, aggregation and analysis, as the data can be collected in public.[252] There have been efforts to bridge the gap and establish best practices for privacy, accountability, and transparency regarding commercial and private drones;[253] however, the best practices guide is voluntary.[254]

B. Wiretap and Recording Laws

The federal wiretap statute governs law enforcement use of wiretaps and pen registers.[255] However, such legislation concerns governments only.[256] Surveillance by private actors such as delivery drones can be subject to state wiretapping laws that share a federal statutory core,[257] or laws against recording in private spaces.[258] State wiretap laws vary as to whether they

---

249 *See* Restatement (Second) of Torts § 652B cmt. c. (Am. L. Inst. 1977) (discussing that there is generally no liability for photographing or observing a person while in public "since he is not then in seclusion, and his appearance is public and open to the public eye"); Scharf, *supra* note 52, at 1104.

250 *See* Daily Times Democrat v. Graham, 162 So. 2d 474, 478 (Ala. 1964) ("To hold that one who is involuntarily and instantaneously enmeshed in an embarrassing pose forfeits her right of privacy merely because she happened at the moment to be part of a public scene would be illogical, wrong, and unjust."); Scharf, *supra* note 52, at 1091.

251 Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998); Villasenor, *supra* note 27, at 501.

252 *See* Scharf, *supra* note 52, at 1096 (discussing the gap between technological advances and privacy torts).

253 NAT'L TELECOMM. & INFO. ADMIN., VOLUNTARY BEST PRACTICES FOR UAS PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY 1 (2016), https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf [https://perma.cc/XPG2-J25C].

254 Scharf, *supra* note 52, at 1096 n. 232.

255 18 U.S.C. §§ 2510-2522 Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

256 *See* DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 168 (2011) ("The Pen Register Act regulates the government's access to routing and addressing information.").

257 Kaminski, *supra* note 105, at 58, 65.

258 *See Id.* at 63 (referring to bills against recording at private farms)*; see also Cattlemen Aiming to Kill Messenger*, S.F. CHRON. (Mar. 22, 2013, 7:38 PM), http://www.dmlp.org/legal-guide/recording-phone-calls-and-conversations [https://perma.cc/J5UE-XB8A] (documenting state legislative efforts to impose criminal penalties on the distribution of videos recorded at farming operations).

require the consent of one party, or all the parties involved[259] in order to establish a reasonable expectation of privacy in the conversation and allow civil action against violators.[260]

Such legislation has limitations. First, it can conflict with the First Amendment rights of the entity that operates the drone recording the private conversations. If the law is too broad and bans an entire medium of expression, courts can strike it down.[261] However, if the law is too narrow, it can be shorthanded to remedy many types of drone invasions. Furthermore, the existing legislation applies to audio recordings only and does not restrict virtual recording and taking pictures from drones. Finally, application of the law is limited to private conversations. Courts consider the location of the conversation and whether it occurred in private or public spaces.[262] Thus, state wiretapping laws would only apply to wiretapping in private homes when there is no doubt of a *reasonable expectation of privacy*,[263] and might apply to "recording from afar" using high-resolution recording systems. However, such laws are less likely to apply to audio recording of drone delivery services in public spaces and the collection and analysis of audio recording for purposes of influencing consumer choices. Consequently, delivery drone audio recording of conversations in public would not require consent.

Even when drones wiretap and record conversations in private spaces, there is no recognized privacy violation if the parties *consented* to the recording of their conversation.[264] As noted, some states do not require consent by all parties.[265] Thus, the person who ordered the delivery drone might consent to the recording by clicking "I agree" in the box under the Terms of Service of the platform that operates delivery drones. However, as this Article has

---

259 *See* Kaminski, *supra* note 105, at 65-66 (explaining that a number of states have all-party consent wiretap laws, accordingly, recording audio private conversations of parties without consent may be subject to arrest or prosecution).

260 Kaminski, *supra* note 105, at 68; *see also Recording Phone Calls and Conversations*, DIGIT. MEDIA L. PROJECT (Sept. 10, 2021), bit.ly/3hh980r [https://perma.cc/S6LU-HQRH] (recommending acquiring consent before recording communications to mitigate the likelihood of civil claims).

261 *See* Kaminski, *supra* note 105, at 6, 69, n. 61 (referring to *Alvarez*, 679 F.3d at 586, 587) (banning all recordings, even those not intended as private did not survive the First Amendment); Christina Murray, *Cameras Down, Hands Up: How the Supreme Court Chilled the Development of the First Amendment Right to Record the Police,* 71 MERCER L. REV. 1125, 1130 (2020). This Article will expand on the First Amendment and Privacy legislation in Part IV.

262 *See e.g.*, State v. Clark, 129 Wash. 2d 211, 225–26 (1996).

263 *See* State v. Kipp, 179 Wash. 2d 718, 732 (2014) (concluding that because the conversation took place in the kitchen of a private home, there is a reasonable expectation to privacy).

264 Kaminski, *supra* note 105, at 68.

265 *See Id.* ("State wiretap laws, for example, vary in whether they require the consent of one party, or the consent of all parties.").

explained, in many cases, such consent is uninformed, flawed and even coerced.[266] Moreover, this consent is also liable to impact on the privacy of third parties that might participate in the conversation.[267] In states where consent by all parties is required, courts might find that there was implicit consent if the parties to the conversation had knowledge that the drone was recording their conversation.

In summary, state wiretapping laws fail to provide a remedy for all types of delivery drone invasions. Wiretapping laws focus on private spaces and generally do not remedy recordings in public and the retention of such recordings. Even within private spaces, consenting to wiretapping might nullify the violation of privacy by delivery drones.

C. Between Airspace Rights and Ownership: FAA Regulation and Trespass

When a delivery drone enters a person's property, flying at a low level without permission, the act can constitute a trespass tort.[268] In June 2016, the FAA announced a plan to integrate drones into the National Airspace System (NAS) and establish a framework for commercial drones.[269] Part 107 raised questions regarding landowner property rights and their ability to exclude drones operated for commercial purposes from the airspace above their land. These questions centered around the operational height restriction.[270] Whereas manned aircrafts are permitted to fly only above 500 feet, the *maximum* height for drones is 400 feet. FAA regulations focus on safety rather than privacy.[271] Furthermore, the FAA denied the petition of a public interest organization focused on emerging privacy issues (EPIC) for a separate public rulemaking on drone privacy issues.[272] The D.C. circuit

---

266 For a comprehensive explanation on the problems with consent, see Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. UNIV. L. REV. 1461, 1462 (2019).

267 *See generally*, Barocas & Levy, *supra* note 203.

268 *See, e.g.*, ARIZ. REV. STAT. § 13-1501 (West 2012); *see also* Bennett, *supra* note 47 ("[A]n unannounced Quadcopter hover, inside a neighbor's back yard barbecue and at hair-parting altitude, could theoretically put a drone operator on the hook for trespassing. This depends on how a state trespassing statute has been written and how far a court is willing to go in interpreting it."); Villasenor, *supr*a note 27, at 499 (explaining that trespassing statutes are worded in a manner that would encompass trespassory use of drones).

269 Tyler Watson, *Maximizing the Value of America's Newest Resource, Low- Altitude Airspace: An Economic Analysis of Aerial Trespass and Drones*, 95 IND. L.J. 1399, 1401 (2020).

270 *Id.*

271 *See* Watson, *supra* note 269 (referring to Operation and Certification of Small Unmanned Aircraft Systems); *see also* Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. at 42,190 (June 28, 2016) ("[T]he FAA notes that its mission is to provide the safest, most efficient aerospace system in the world, and does not include regulating privacy.").

272 Scott, *supra* note 232, at 775.

court denied EPIC's petition to review the agency's failure to consider privacy in the context of the small drone rulemaking, concluding it was premature.[273] Since FAA regulation does not regulate privacy, states must interpret their existing laws and determine whether they provide adequate legal protection to property owners against drone intrusion.[274]

Although FAA regulation does not regulate privacy, it regulates airspace rights affecting privacy by limiting intrusion through the tort of trespass. How does the law balance airspace rights and ownership? Historically, landowners held property rights over the surface of the land and over the airspace above the land, "stretching indefinitely up to the sky."[275] This old English doctrine remained the law until the Supreme Court's holding in *United States v. Causby* recognizing that "[t]he airplane is part of the modern environment of life, and the inconveniences which it causes are normally not compensable."[276] The Court justified Congress's declaration that the navigable airspace is a "public highway" because otherwise, private claims to the airspace would seriously jeopardize public interest. According to *Causby*, navigable airspace includes all airspace 500 feet above public airspace.[277] The Court was less clear about who owned the airspace below 500 feet, stating that landowners held exclusive rights to airspace within the "immediate reaches" of their land.[278] However, the Court did not determine the boundaries of the "immediate reaches."

Drones operate closer to the ground than manned aircrafts, as the FAA has determined that drones should be operated in low-altitude airspace, away from manned aircraft. This raises the question whether drones fly within the immediate reach of land owners and whether they commit a tort of trespass. In aerial trespass cases, "[f]light by [an] aircraft in the air space above the land of another is a trespass if, but only if, (a) it enters into the immediate reaches of the air space next to the land, and (b) it interferes substantially with the other's use and enjoyment of his land."[279] Such a doctrine creates an ambiguity regarding landowner property rights. The rights are treated more like a nuisance claim suit than a "right to exclude" and the condition

273 *Id.*; EPIC v. FAA, 821 F.3d 39 (D.C. Cir. 2016). Scott argues that the FAA should regulate privacy issues. Scott, *supra* note 232, at 791.

274 Watson, *supra* note 269, at 1401.

275 *Id.* at 1402.

276 United States v. Causby, 328 U.S. 256, 266 (1946).

277 Watson, *supra* note 269, at 1403.

278 *Id.* (referring to *Causby*, 328 U.S. at 264).

279 Restatement (Second) of Torts § 159(2) (Am. L. Inst. 1965); Watson, *supra* note 269, at 1403.

"interferes substantially with the landowner's enjoyment of the land" is unclear.

In order to provide more clarity and uniformity, in July 2018, the National Conference of Commissioners on Uniform State Laws discussed a proposed per se aerial trespass rule[280] to hold drone operators liable for nuisance damages when flying below 200 feet.[281] Companies that operate drones criticized the proposal arguing that it gives landowners an absolute right to exclude drones, creates an "inflexible line in the sky" that is inconsistent with tort law on aerial trespass, and that there is no need for a law to restrict an activity that does not cause cognizable harm.[282] Companies further argued that the proposed per se rule would lead to costly litigation and fail to strike an appropriate balance between innovation and privacy.[283] Scholarship sided with keeping the doctrine of drone trespass flexible. The Supreme Court's decision in *Causby* supports flexibility as it takes into account "substantial interference" with use and enjoyment of land. This is an economic consideration that is equivalent to that of nuisance.[284] Thus, it was proposed that every state should define the maximum permissible height as appropriate based on a broad geographic classification system of rural, urban, suburban, and agricultural airspace, and design flexible liability rules.[285]

We believe that a flexible approach to trespass is superior to a per-se rule that would hinder innovation and development of drones.[286] However, be it a per-se rule or a flexible scheme, the doctrine of trespass is insufficient to address most of the privacy concerns posed by delivery drones, as it focuses only on invasion of privacy at home and on "looking from afar" and fails to provide a remedy for invasion of privacy in public as well as the collection and analysis of information, the possibility it may be used to influence consumer choices as there is no trespass in such circumstances.

---

280 Watson, *supra* note 269, at 1404.

281 *Id.*

282 *Id*. at 1405.

283 *Id*. at 1406.

284 *Id*. at 1412.

285 *Id.* at 1433.

286 For further analysis with regards to how best to regulate new technologies that have not yet matured, see Nissim Cohen & Hadar Jabotinsky, *Nudges and Sludges: Regulating Innovation* (Jan. 22, 2020) (unpublished manuscript), papers.ssrn.com/sol3/papers.cfm?abstract_id=3523910.

D. Specific State Law Regarding Civilian Drones

There are positive considerations supporting the regulation of invasions of privacy by commercial drones by state law rather than federal law. State laws draw on the state's approach to privacy regulation governing civilian drone use as well as on the state's experience regulating other forms of civilian-on-civilian surveillance.[287] Although some policy makers have called for a robust federal approach to drones and privacy,[288] currently private and commercial drone surveillance is regulated primarily by state law. State law focuses on three categories: first, common law protections against non-governmental intrusion by the law of trespass; second, privacy civil torts and state wiretap laws; and third, civil and criminal laws designed specifically to block unwanted aerial surveillance by privately owned drones.[289]

Different states define drone surveillance in different ways. For example, Tennessee enacted two privacy statues. One makes video drone surveillance of citizens that lawfully hunt or fish a criminal offense.[290] Another law prohibits, with exceptions, the use of an "unmanned aircraft to capture an image of an individual or privately owned real property . . . with the intent to conduct surveillance on the individual or property captured in the image," and to retain or publicize the images.[291] Wisconsin's drone law outlines a narrower scope of invasion. Accordingly, a private individual would commit a criminal offense when using a drone to "photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy."[292] The Texas Privacy Act bans drone photography of individuals in private property without the consent of the property owner.[293] Idaho restricts any "person or entity" from using a drone to photograph individuals for the purpose of publishing or publicly disseminating the images, without their consent.[294] In Nevada, the law

---

287 Kaminski, *supra* note 105, at 66.

288 Bennett, *supra* note 47, at 1. The FAA's regulations focus on safety rather than privacy that is regulated by state law. *See* Watson, *supra* note 269, at 1401 ("[T]he FAA's regulations focus on safety rather than privacy . . . .").

289 Bennett, *supra* note 47, at 3–4.

290 TENN. CODE ANN. § 70-4-302(a)(6) (West 2014); Bennett, *supra* note 47, at 4.

291 TENN. CODE ANN. § 39-13-903(a)(1) (West 2014 & Supp. 2017). For further information, see Scharf, *supra* note 52, at 1099.

292 WIS. STAT. ANN. § 942.10 (West 2018); Scharf, *supra* note 52, at 1099; Bennett, *supra* note 47, at 4.

293 H.B. 912, 83d Leg. (Tex. 2013) § 423.003; Kaminski, *supra* note 105, at 60; Philip R. Thomas & Timothy T. Takahashi, *The Wild West of Aviation: An Overview of Unmanned Aircraft Systems Regulation in the United States*, AIAA SCI TECH 2020 FORUM 6-10, at 10 (Jan. 2020).

294 *See* Scharf, *supra* note 52, at 1098, referring to IDAHO CODE § 21-213 (2018) (creating a civil cause of action against any person in violation of this statute).

creates a cause of action for drone flights over private property, without permission through a trespass-based statute.[295] Florida even drafted a criminal statute to prohibit the use of drones that interfere with an individual's reasonable expectation of privacy.[296]

Existing statutory schemes regarding drone surveillance vary in scope of protection. Such laws provide some relief for invasions of privacy arising from the use of drone technology. Yet, a private individual has not yet brought a sustainable case alleging a violation of privacy due to nongovernmental drone use.[297] Moreover, the laws reviewed above focus on privacy at home, "looking from afar," and in rare cases provide relief against drone invasions of privacy in public when the photos, videos and recordings are disseminated in public. The aspects of collection, aggregation and utilization of private information for profits are neglected in state drone legislation.

E. Sectorial Information, Privacy and the New Approach of the California Consumer Privacy Act

The American constitutional system has no explicit constitutional right to privacy. Constitutional law protects privacy from the government, and is characterized by negative rights against the state. There are very few constitutional rights that apply to private actors.[298] Furthermore, laws in the U.S. focus on negative privacy and are short handed in addressing information privacy. In contrast to the EU omnibus privacy under the framework of the General Data Protection Regulation ("GDPR"),[299] which applies to all personal data irrespective of the sector in which it was collected (this Regulation will be addressed in detail in Part III below), the U.S. lacks

---

295 Scharf, *supra* note 52, at 1098, referring to NEV. REV. STAT. ANN. § 493.103 (LexisNexis 2012 & Supp. 2016).

296 *See* Scharf, *supra* note 52, at 1098, referring to FLA. STAT. ANN. § 934.50 (West 2015 & Supp. 2019) ("For purposes of this section, a person is presumed to have a reasonable expectation of privacy on his or her privately owned real property if he or she 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 their with the use of a drone."). .

297 Scharf, *supra* note 52, at 1100.

298 Neil Richards & Woodrow Hartzog, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1727 (2020).

299 Regulation (EU) 2016/679 of the European Parliament and the Council of April 27, 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).

a comprehensive federal data privacy law.[300] Categorically, the American approach towards information privacy and data protection is sectoral.[301] Federal law is directed towards specific industries or sensitive contexts. For example, children under twelve who use the Internet are protected under the Children's Online Privacy Protection Act (COPPA).[302] There are also sector-specific federal laws, such as: the Fair Credit Reporting Act ("FCRA"),[303] which focuses on companies that compile individual credit scores; the Health Insurance Portability and Accountability Act ("HIPAA"), which focus on health care data[304]; and the Gramm-Leach-Bliley Act,[305] which focuses on financial information and similar sectorial privacy laws.[306] These sectorial federal privacy laws apply in narrow domains.

However, the State of California recently passed the California Consumer Privacy Act ("CCPA"),[307] which entered into force in January 2020, establishing omnibus privacy protections. Until the CCPA, no state or federal statute in the U.S. imposed privacy protections across all industry sectors.[308] Entities could by default collect and use personal data as they wished.[309] The CCPA changed this regarding companies (as opposed to

---

300 Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law,* 105 MINN. L. REV. 1733 (2021). (2019).

301 A sectoral approach is contrary to an omnibus approach that regulates privacy consistently across all industries and contexts. For more on these differences, see Daniel Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, TEACHPRIVACY (Nov. 13, 2015), teachprivacy.com/problems-sectoral-approach-privacy-law.

302 15 U.S.C. §§ 6501–6506 (2018).

303 Fair Credit Reporting Act of 1970 (FCRA), Pub. L. No. 91–508, 84 Stat. 1114 (codified as amended at 12 U.S.C. § 1830).

304 The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104-191, 110 Stat. 1936; 45 C.F.R. § 164.514(b)–(c) (2019).

305 Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 USC).

306 Neil M. Richards, Andrew Serwin & Tyler Blake, *Understanding American Privacy*, in RESEARCH HANDBOOK ON PRIVACY AND DATA PROTECTION LAW: VALUES, NORMS AND GLOBAL POLITICS 50-72 (Gloria González Fuster et al. eds.) (2022), papers.ssrn.com/sol3/papers.cfm?abstract_id=3256918.

307 CAL. CIV. CODE §1798.198(a) (Directly regulating data brokers independent of their commercial relationships). For further information, see Chander et al., *supra* note 300, at 1734.

308 Chander et al., *supra* note 300 at 1738. However, it should be noted that after the CCPA came into force more states followed its footsteps. *See e.g.,* Virginia's Consumer Data Protection Act (VCDPA), S.B. 1392 (2021). For further information, see Daniel J. Solove, *The Limitations of Privacy Rights* (manuscript at 9).

309 Eric Goldman, *An Overview of the California Consumer Privacy Act*, 1-2 (June 2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3211013.

individuals) that do business in the State of California, [310] collect consumer personal data,[311] and determine the means and purposes of processing.[312]

The CCPA defines personal data broadly as information that is "capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[313] It promotes transparency regarding that personal data as it gives consumers the right to know what personal information is collected about them, whether it is sold or disclosed and to whom.[314] It also grants consumers access rights and allows them to request the categories and specific pieces of personal information the business has collected on them.[315] The CCPA also grants a right to opt out, to say no to data sales,[316] and outlines the right to delete information.[317]

This Act is likely to push other states to improve their legislation as well.[318] In fact it has already influenced at least fourteen states to introduce similar data protection bills.[319] More states are considering enacting comprehensive data privacy bills in the near future.[320] CCPA is also likely to encourage large U.S. companies to revise their privacy policies for all states in order to avoid having one standard for California which conflicts with privacy policies in

---

310 *Id.* at 21.

311 CAL. CIV. CODE §1798.140(d), (e).

312 Eric Goldman, An Introduction to the California Consumer Privacy Act (CCPA) 1-2, (July 2020) (unpublished manuscript); *see also* Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L REV. 365, 403-05 (2019) (citing Daisuke Wakabayashi, *Silicon Valley Faces Regulatory Fight on Its Home Turf,* N.Y. TIMES (May 13, 2018), https://www.nytimes.com/2018/05/13/business/california-data-privacy-ballot-measure.html [https://perma.cc/9CKP-9HZW] ("It gives consumers the right to ask companies to disclose what data they have collected on them; the right to demand that they not sell the data or share with third parties for business purposes; and the right to sue or fine companies that violate the law.").

313 CAL. CIV. CODE § 1798.140(v)(1).

314 *See* Chander et al., *supra* note 300, at 15, referring to Cal. A.B. 375 Sec. 2(i) (explaining that the CCPA intends to give consumers "'[t]he right…to know what personal information is being collected about them,' and '[t]he right…to know whether their personal information is sold or disclosed and to whom.'").

315 Goldman, *supra* note 312, at 3; Chander et al., *supra* note 300, at 16; CAL. CIV. CODE §§ 1798.100(a), 1798.110(a).

316 Goldman, *supra* note 312, at 5; Rustad & Koenig, *supra* note 312, at 403; Chander et al., *supra* note 300, at 17; CAL. CIV. CODE § 1798.120.

317 *See* CAL. CIV. CODE § 1798.105(a) (explaining that upon a consumer's request, a business shall delete any personal information about the consumer that the business collected from the consumer. Note, however, that this does not apply to third parties); Chander et al., *supra* note 300, at 18.

318 Chander et al., *supra* note 300, at 9-10, 39-41.

319 *See* Richards & Hartzog, *supra* note 298, at 1691 (citing Mitchell Noordyke, *U.S. State Comprehensive Privacy Law Comparison*, INT'L ASS'N OF PRIVACY PROFS. (Apr. 18, 2019), iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/).

320 *See* Chander et al., *supra* note 300, at 31 ("[A]t least 17 states, in addition to California and Puerto Rico, that considered or enacted comprehensive data privacy laws in 2018 and 2019.").

other states.[321] However, the CCPA does not treat privacy as a fundamental right in the way EU data protection laws do. It is "a transactional privacy law concerned with protecting *consumers* in their dealings with *commercial* entities."[322] It focuses on transparency regarding collection and uses of personal information and does not impose substantive duties on companies.[323] Unlike the EU approach (described below in Part III of this Article), it does not restrict data collection, allowing for-profit companies to gather and retain information on individuals.[324] The CCPA grants individuals only two limited rights–to opt out of sale and to request deletion[325]–and it does not require the data subject's consent for companies to process their information in the first place.[326] This opt-out approach leaves gaps in information privacy protection against invasion of privacy by commercial delivery drones, affording individuals little control over their personal information. Most individuals cannot fully grasp the conclusions that companies operating delivery drones can reach based on their information. Consequently, they are likely to find it difficult to assess risks and are less likely to opt-out or request to delete the information that drones collect on them.[327] Moreover, even when individuals opt out, and when they recognize violations of information privacy by a company operating in California, under the CCPA, there is no private right of action for affected individuals to enforce most elements of the law.[328]

In summary, the current U.S. legal regime regarding invasion of privacy as it stands is insufficient to protect individual privacy in the age of modern

---

321 Rustad & Koenig, *supra* note 312, at 405.

322 Chander et al., *supra* note 300, at 19.

323 *Id*. at 20.

324 *See Id.* at 21 ("The CCPA lacks the GDPR's affirmative regulatory requirements—ranging from data minimization to risk assessments to recording requirements—imposed on companies even where there is not a corresponding individual right.").

325 *See* Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 COLO. L. REV. 593, 599 (2019) (explaining that the default for U.S. internet transactions is that if the data subject has not opted out of an online tracking service, then that natural person's data can be resold to third parties. In contrast, the EU GDPR requires the data subject to opt in; that is, to grant limited written consent before the internet intermediary can post the information); Chander et al., *supra* note 300, at 18 ("While the CCPA's broad definition of personal data, emphasis on transparency, and establishment of some individual rights do go further than previous U.S. law, however, none of these shifts goes nearly as far as the GDPR."); *Id.* at 19 ("[I]t shares the presumption of most other American privacy law that personal data may be collected, used, or disclosed unless a specific legal rule forbids these activities.").

326 *See* Chander et al., *supra* note 300, at 19 (explaining that the right of private action exists only for data breaches). *See* California Consumer Privacy Act of 1018, AB 375.

327 Solove, *supra* note 171, at 1.

328 Chander et al., *supra* note 300, at 21.

complex drone technology.[329] Although privacy laws generally protect privacy at home and in many cases even invasions "looking from afar," there is a lack of privacy protection in public spaces as well a lack of protection against mass data collection and aggregation. The lack of privacy protection in the public space exposes the public to potential mass surveillance by the private sector. This personal information can be sold and can even reach the government, which can use it without a warrant.[330] In the past, it was difficult to collect, analyze and retain mass data on individuals in the long term. Thus, large-scale surveillance in public spaces was a minimal concern as information on individuals in public remained obscured. Technological developments and drones in particular, have reduced obscurity in public, allowing for mass surveillance,[331] collection of information and utilization thereof for commercial profit. Privacy theories that focus on privacy as a negative right and the right to be let alone fail to address mass data collection. Regulation based on such theories is ill-equipped to protect information privacy and remedy the harm of such large-scale surveillance. Therefore, a more comprehensive framework should be set forth.

III. TOWARDS A NEW FRAMEWORK AND GUIDELINES FOR REGULATING INVASION OF PRIVACY BY DELIVERY DRONES

This Part argues that limitations on invasions of privacy at home and "looking from afar" should play a role in protecting the negative right to privacy. However, affirmative duties that address the violation of information privacy are the key to protecting against drone surveillance in public and platform opportunism. This Part will describe a lesson that can be learned from the EU GDPR,[332] which was implemented specifically in the context of drones in the EU commercial drone regulation.[333] As the EU regulation leads the world in the field of data protection, much can be learned from it. This Part will then address the new approach of leading U.S. scholarship regarding privacy, which advocates "redefining privacy as

329 *See generally* Scharf, *supra* note 52 (referring to common law privacy torts, however valid to all the laws overviewed).

330 Scott, *supra* note 232, at 785.

331 *Id*. at 787.

332 GDPR, *supra* note 56.

333 Parliament and Council of the European Union Regulation 2018/1139, 2018 O.J. 2 (L 212) (On common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations).

a matter of 'trust'"[334] or as a loyalty and fiduciary like duty.[335] Such duties can supplement a data protection regime that might apply even when the subject has no formal relationship with the data subject, as in the case of data brokers.[336] Following the overview of EU regulations and the connected U.S. relational approach, this Part will conclude with concrete guidelines and duties for delivery drones that accommodate the challenges delivery drones pose to privacy.

A. The EU General Data Protection Regulation (GDPR)

Data protection is enshrined as a fundamental right in the European Convention on Human Rights and the EU Charter.[337] The EU's GDPR[338] is a model of omnibus privacy. The Regulation covers all personal data, regardless of the sector in which it was collected, and it protects the personal data of all "natural persons."[339] The Regulation imposes uniform obligations on collection, processing or transferring personal data, through inclusive definitions of "data controllers" and "data processors."[340] It applies in all contexts and is not restricted to the commercial consumer-client relationship. Like earlier data protection directives, it prohibits the processing of sensitive categories of personal data, except where specific conditions apply, such as *explicit consent* by the data subject.[341]

One of the primary provisions stipulated by the GDPR is *data minimization* (collecting no more data than necessary for those purposes), as it restricts personal data processing to data "collected for specified, explicit and

---

334 Chander et al., *supra* note 300, at 37.

335 *See generally* Richards & Hartzog, *supra* note 58; Balkin, *supra* note 59.

336 Richards & Hartzog, *supra* note 58, at 62.

337 EUR. CONSULT, European Convention on Human Rights, art. 8; Charter of Fundamental Rights of the European Union: 2000 O.J., arts. 7, 8; Chander et al., *supra* note 300, at 1747 ("Data protection laws like the GDPR proceed from the principle that data protection is a fundamental human right safeguarded through constitutional protections in the European Convention on Human Rights and the EU Charter.").

338 GDPR, *supra* note 56.

339 GDPR, *supra* note 56, at art. 1(1).

340 Chander et al., *supra* note 300, at 13.

341 *See* Parliament and Council of the European Union Directive 95/46, art. 8, 1995 O.J. (L 281) (Referring to special categories of data); Parliament and Council of the European Union Regulation 2016/679, arts. 9-10, 2016 O.J. (L 119/1) (referring to processing of special categories of personal data such as race, political opinion, information about health and to processing of personal data relating to criminal convictions and offences). For further information, see Chander et al., *supra* note 300, at 20 ("The GDPR strives to do so by requiring stringent forms of consent in a number of circumstances and by granting individuals robust rights throughout the life cycle of data processing.").

legitimate purposes and not further processed in a manner that is incompatible with those purposes. . . ."[342] Companies cannot process information beyond the purpose of collection. They are required to inform users of new purposes for processing, must obtain user *consent* for commercializing their private data and enable them to withdraw that consent.[343] The GDPR outlines norms of *limitation* on the duration of *data retention* by commercial actors of personally identifiable information.[344] It also grants all data subjects a *right of access* to their personal data.[345] Furthermore, companies that control the data must inform data subjects of their rights to rectify, to erase, and to allow the data subject correction of inaccurate information. Article 17 provides a *right to erasure ('right to be forgotten')*,[346]obligating data controllers to delete data that is no longer required for the purposes for which it was collected or processed.[347] Another right provided to data subjects is the *right to object to data processing and profiling*, at any time. If the purpose of data processing is *direct marketing*, the data subject possesses an absolute right to object.[348] In addition, data subjects

342 GDPR, *supra* note 56, at art. 5; Chander et al., *supra* note 300, at 1756.

343 GDPR, *supra* note 56, at art. 6-7; *see* Tsesis *supra* note 325, at 596 (explaining GDPR's consent requirements).

344 *See* GDPR, *supra* note 56, art. 5(e) (explaining that data should only be retained for as long as is required to achieve the purpose for which it was collected and processed, unless they need to be retained "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes"); *see* Tsesis, *supra* note 325, at 594 (discussing the GDPR limitation requirement).

345 GDPR, *supra* note 56, at art. 15 ("Right of access by the data subject").

346 GDPR, *supra* note 56, at art. 17; *see* Lilian Edwards & Michele Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 67-69 (2017) (discussing the right to erasure in the context of machine learning); Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65, 90 (2019) ("Roughly summarized, a data subject has a right to erasure when he or she successfully exercises the right to object, when the personal data were unlawfully processed, should be erased because of a legal obligation, or are no longer necessary in relation to the processing purposes."); Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, the Right to be Forgotten, and the Construction of the Public Sphere*, 67 DUKE L. J. 981 (2018) (analyzing the right to be forgotten in the context of the *Google Spain* case); Tsesis, *supra* note 325, at 602 (describing the right erasure as "[t]he most important development for data privacy in 2018. . . .")

347 *See* Tsesis, *supra* note 325, at 603 (explaining the requirement to delete data that is no longer necessary).

348 GDPR, *supra* note 56, art. 21(1)-(3); *see* Sandra Wachter, *Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR*, 34 COMPUT. L. & SEC. REV., 436, 443 (2018) (explaining that in all other cases data processing must stop, unless the data controller can demonstrate compelling legitimate interests that override the interests of the data subjects); *see also* Michele E. Gilman, *Five Privacy Principles (from the GDPR) the United States Should Adopt To Advance Economic Justice, 52* ARIZ. ST. L.J. 368, 413 (2020) (discussing the broad conception of privacy on which the GDPR is based).

hold a right not to be subject to decisions based solely on automated processing.[349] Data processors can however evade this requirement by involving a human in the process (human in the loop).[350]

The Regulation also stipulates "*data protection by design and default*", which provides that the creation of privacy-friendly systems must commence at the design stage.[351] Thus, controllers must, at the time systems are developed as well as at the time of actual processing, implement "appropriate technical and organizational measures" in order to to "protect the rights of data subjects." In particular, "data protection by default" is required so that only personal data necessary for processing are gathered.[352] Common applications of data "protection by design are anonymization and pseudonymization of personal data, minimization of data during processing and storing data, storage limitation, transparency regarding processing and limited access to personal data."[353]

In addition, the EU legislation stipulates affirmative data controller obligations, and expands individual rights over personal data. Individuals possess private rights of action regarding their data. National data protection regulatory authorities possess enforcement authorities. Efforts between national authorities are coordinated through the European Data Protection Board.[354]

The GDPR applies to drones that collect information for commercial platforms. Privacy and data protection enhancing recommendations regarding drones were however proposed even before the GDPR. Furthermore, the EU has legislated a specific regulation on drones, which applies principles set down in the GDPR principles, as outlined in the following subsection.

---

349 *See* GDPR, *supra* note 56, art. 22 (explaining that this prohibition applies only when the decision is "based solely" on algorithmic decision-making); *see also* Margot E. Kaminsky, *The Right to Explanation, Explained*, 34 BERKELEY TECH. L.J. 189, 196-98 (2019) (discussing article 22 of the GDPR and the related exceptions).

350 *See* Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1016 (2017) ("[O]nce the process is not 'solely' automated, this provision will not apply.").

351 Art. 25 GDPR.

352 GDPR, *supra* note 56, art. 25; Michal Lavi, *Publish, Share, Re-Tweet, and Repeat*, 54 U. MICH. J.L. REFORM 441, 495 (2021).

353 Oliver Vettermann, *Self-Made Data Protection—Is it Enough? Prevention and After-care of Identity Theft*, 10 EUR. J.L. TECH. § 4.2 (2019).

354 Chander et al., *supra* note 300, at 22.

B. Specific EU Regulation for Commercial Drones – Applying the GDPR

As early as June 2015, before the GDPR entered into force, the European Data Protection Board (EDPB) (formerly Article 29 Working Party), an EU body charged with the application of the GDPR,[355] issued an Opinion on Privacy and Data Protection relating to the Utilization of Drones. The opinion addresses risks to individual privacy and civil and political liberties resulting from opening the aviation market to drones.[356] It includes recommendations to consider the purpose of the operations and the type of drones and evaluate data protection. It proposed the adoption of suitable "privacy by design and by design default" measures for services and products to avoid collection and processing of unnecessary personal data.[357] Other recommendations to drone operators included: (1) to choose proportionate technology and suitable default privacy measures, and set services and products to avoid unnecessary collection and processing; (2) provide advance notice to those who might be impacted by the data processing; (3) adopt security standards and prevent unauthorized processing; (4) delete or anonymize any unnecessary personal data soon after collection or as soon as possible; (5) embed privacy enhancing design and policy; (6) involve a Data Protection Officer in the design and implementation of policies related to the use of drones; (7) avoid flying near private buildings.[358] Such guidelines are even more relevant after the GDPR entered into force.

In addition to the above guidelines, in July 2018, the EU Parliament and the European Council legislated a specific framework for drones,[359] providing the EU Aviation Safety Agency with additional powers to regulate the use of drones under 150 Kg. This Regulation set down basic rules for unmanned aircrafts and the EU Commission was tasked with setting the technical and operational details. The European Aviation Safety Agency (EASA) has issued an opinion (Opinion No. 01/2018) proposing to develop the legislative framework. EASA proposed that the European Commission

355 *See What is the European Data Protection Board (EDPB)?*, EUROPEAN COMM'N, (last visited Feb. 8, 2022), https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-european-data-protection-board-edpb_en [https://perma.cc/Q3YJ-CSA] (explaining that the EDPB "will help ensure that the data protection law is applied consistently across the EU and work to ensure effective cooperation amongst DPAs").

356 *See* De Schrijver, *supra* note 27, at 351 (discussing the June 2015 Opinion on Privacy and Data Protection Issues relating to the Utilization of Drones).

357 *Id.* at 350.

358 *Id.* at 351-52.

359 Council Regulation 2018/1139, 2018 O.J. (L 212).

adopt a delegated act regarding market product legislation and technical requirements and implement an act regulating drone usage and registration.[360] The EU adopted the proposed regulation providing basic principles regarding safety, security privacy and data protection.[361]

Article 132(1) of Council Regulation 2018/1139refers to data processing. Under this Article, "Member States shall carry out their tasks under this Regulation in accordance with the national laws, regulations or administrative provisions in accordance with Regulation (EU) 2016/679."[362] In fact, this specific Regulation implements GDPR principles in order to protect against the threat drones pose to privacy and data protection by collecting, identifying, or identifiable information. It adopts all risk prevention measures in the GDPR.[363]

The implementing regulation[364] provides detailed requirements that enable assessment of the risks drone technology poses to data protection, as well as the factors drone operators should take into account to reduce the uncertainty of drones. These factors might include the target level of safety, the risks of drone operation, identifying risk mitigation measures and information on the necessary level of mitigating measures.[365] For example, a drone with high-resolution cameras can accurately capture the facial features of data subjects and other identifying information. Therefore, it poses a great risk to data protection, while a drone equipped with low-resolution cameras might not collect any personal information at all.[366]

The GDPR and the Regulation applying it to drones mitigate high risks of drone surveillance.[367] As explained, they apply the principles of data

---

360 De Schrijver, *supra* note 27, at 342.

361 *See* De Schrijver, *supra* note 27, at 342 (discussing the Commission Delegated Regulation); Commission Delegated Regulation 2019/945 of 12 March 2019, Unmanned Aircraft Systems and on Third-country Operators of Unmanned Aircraft Systems, 2019 O.J. (L 152) pp. 1-40; Commission Implementing Regulation 2019/947 of 24 May, 2019, Rules and Procedures for the Operation of Unmanned Aircraft, 2019 O.J. (L 152) pp. 45-71 (the implementing regulation).

362 Council Regulation 2018/1139, art. 132(1), 2018 O.J. (L 212).

363 *See* Eleonora Bassi, et al., *The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management*, 29 MINDS AND MACHINES 579, 581 (2019) ("On the one hand, Article 132 of Reg. (EU) 2018/1139 adopts all the risk prevention measures set up by the GDPR.").

364 Commission Implementing Regulation 2019/947 of 24 May, 2019, Rules and Procedures for the Operation of Unmanned Aircraft, 2019 O.J. (L 152)

365 Bassi et al., *supra* note 363, at 582.

366 *Id.* at 584.

367 *See* De Schrijver, *supra* note 27, at 350 ("The GDPR is applicable to processing of personal data via drones, either by private or public entities for purposes other than law enforcement.").

minimization[368] and privacy by design,[369] taking into account privacy and data protection through the engineering process. Applying the GDPR to drones through drone regulation mitigates harm to information privacy. For example, under these principles, drone flights that do not require personal data to execute their task would not use high-resolution cameras. They would opt for paths that reduce collection of personal data,[370] and be equipped only with devices that are proportionate to their specific purpose: delivering parcels. Alternatively, they should contain software that automatically blurs facial features and avoid retaining them after completing the specific task.[371] Such regulation limits the ability of companies to engage in profiling of existing and potential consumers, reducing data driven influence and manipulation of consumers and third parties.

C. The U.S. Approach to Consumer Protection and the New Concept of Trust

Unlike the EU, the American constitutional system does not include an explicit constitutional right to privacy.[372] Most U.S. laws focus on the transactional consumer protection model. This model governs direct interaction and the company-consumer relationship. It does not include protections that follow the data, similar to the EU regime. Instead, it often relies on a (naive) premise that disclosure and a right of refusal ("notice and choice") are the key to privacy protection.[373]

In recent years, scholars have begun to recognize the shortcomings of U.S. law with respect to information privacy protection,[374] as U.S. law ignores the problem of tech company opportunism. Traditional approaches focus on protecting consumers through transparency about company data practices and users control over their personal information. Scholars have

368 *See* GDPR, *supra* note 56, art. 5(1)(c) ("[Personal data shall be] adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation').").

369 Bassi et al., *supra* note 363, at 6.

370 *See* GDPR, *supra* note 56, art. 25 (describing the data protection by design and by default requirement).

371 *See* De Schrijver, *supra* note 27, at 350 (explaining that this is what the Belgian Data Protection Authority advises to drone operators).

372 *See* Richards & Hartzog, *supra* note 298, at 1727 ("The American constitutional system has no explicit constitutional right to privacy."); Y.B. Eur. Conv. on H.R. art. 7-8 ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

373 Chander et al., *supra* note 300, at 13.

374 *See* Bamberger & Mayse, *supra* note 154 (proposing to learn lessons from Jewish law and shifts the focus from the individual's control over their information to the prohibition of widespread surveillance and big data harms).

recognized that this approach is insufficient to protect privacy, and cannot stop surveillance capitalism manipulation.[375] To account for harm to information privacy, scholars have argued that U.S. law should redefine privacy as "trust,"[376] fiduciary or a duty of loyalty borne by large-scale collectors.[377]

Although these scholars recommend incorporating elements of data protection, such as restrictions on processing, into the U.S. framework, they argue that data protection duties are mainly procedural. Such duties focus on the data and allow collection and processing if the data subject has expressed meaningful consent. In the digital context, consent is a weak protection,[378] that fails to address other privacy values that go beyond individual goods.[379] Moreover, "wherever consent is operable in the information economy, it is both a weapon of data extraction and a shield against accountability" because it legitimizes privacy violations.[380] Focusing on data is thus insufficient to protect privacy. Scholars have proposed that a

---

375 *See* Richards & Hartzog, *supra* note 58, at 17 ("We explain how the failures of American privacy law have enabled corporate opportunism and manipulation of consumers using human information.").

376 The importance of trust in relationships of companies with stakeholders is gaining recognition in recent years. For further information, see SANDRA J SUCHER & SHALENE GUPTA: THE POWER OF TRUST: HOW COMPANIES BUILD IT, LOSE IT, REGAIN IT (2021). The concept of trust gained particular importance in the field of privacy, regarding relationships of digital companies with their users. *See* ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 9 (2018) (explaining that digital companies should adopt norms of trust they should neither breach user trust nor take actions that users would reasonably consider unexpected or abusive for digital companies to do); Bamberger & Mayse, *supra* note 154, at 13 (learning a lesson from Jewish law that is in line with moving from an oppositional model to one relieving frictions in relationships by promoting sustainable trust).

377 *See* Chander et al., *supra* note 300, at 37 (explaining that the concept of trust, fiduciary or loyalty is an emerging strain of thought about privacy among US scholars); Balkin, *supra* note 59, at 11 ("[T]he law should treat digital companies that collect and use end user data according to fiduciary principles."); Richards & Woodrow, *supra* note 58, at 36 (referring to loyalty duties); *See also* CARISSA VELIZ: PRIVACY IS POWER: WHY A D HOW YOU SHOULD TAKE BACK CONTROL OF YOUR DATA 164-67 (2020).

378 Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U.L. REV. 961, 967 (2021) (describing the ability of companies to exploit data through notice provisions) ("Put simply, a legal model grounded in "notice and choice" cannot prevent data-based manipulation when notice is fictional, when choice can be manufactured by the tools of data and behavioral science, and when rules for individuals are used to regulate a problem with social dimensions."). *See also* Daniel J. Solove, The Limitations of Privacy Rights (manuscript at 21) ("With the notice-and-choice approach, the right to information is twisted into serving a pernicious purpose – to legitimize nearly any form of data collection and use through an implausible fiction of consent.").

379 *See* Richards & Hartzog, *supra* note 144 at 991.

380 Ari Ezra Waldman, *Practice Performance and Privacy Law*, 110 CALIF. L. REV. 1221, 1257 (2022).

framework for information privacy should move one step further.[381] Privacy should be built on trust rather than merely protecting against invasion.[382] It should not be based on consent to invasion. Instead, an obligation of good faith and non-manipulation should be prescribed.[383]

Information fiduciaries are a classic example of the concept of trust. The digital company's obligations towards its users' information can be compared to the fiduciary duties of doctors or lawyers towards patients and clients.[384] Digital companies can be likened to fiduciaries because, much like lawyers and doctors, they receive—and even actively collect—personal information on the individuals that use their services and they are trusted to treat this information with care.[385] Users have little knowledge about the digital company, its operations, the data it collects, how data is used, and how data is shared.[386] Due to this asymmetry, users are particularly vulnerable and naively trust the companies, believing they will not betray their trust or manipulate them. Therefore, Professor Jack Balkin has argued that the law should impose duties of care, confidentiality, and loyalty upon such companies, limiting how they can profit from their users and beneficiaries.

"The nature of the fiduciary obligation depends on the nature of the relationship" and the potential risk for abuse by the more powerful party in

---

381 *See* Richards & Hartzog, *supra* note 298, at 1760 ("[A] comprehensive model is the best path forward. This would include fundamental elements of data protection, such as default prohibitions on data processing and data subject rights, but it would not purely be defined by the limited data protection model. Instead, the comprehensive model could incorporate relational rules built around loyalty and care . . . .").

382 *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV., 431, 462-65 (2016) (arguing the foundation of privacy should be trust).

383 *See* Jack M. Balkin, *Fixing Social Media's Grand Bargain* 14, HOOVER WORKING GRP. ON NAT'L SEC., TECH. & L., (2018) [hereinafter Balkin, *Grand Bargain*] ("Contractual models will prove insufficient if end users are unable to assess the cumulative risk of granting permission and therefore must depend on the good will of data processors. The fiduciary approach to obligation does not turn on consent to particular transactions . . . .").

384 *See Id.* at 12 ("As information fiduciaries, digital companies should have duties of care, confidentiality, and loyalty toward the people whose data they collect, store, and use."); Jack M. Balkin, *To Reform Social Media, Reform Informational Capitalism in Social Media, Freedom of Speech and the Future of Our Democracy* (forthcoming 2022) (manuscript at 129), http://dx.doi.org/10.2139/ssrn.3925143 [https://perma.cc/8KPJ-UZY4] ("Fiduciary duties apply not only to social media companies, but to any companies that collect and monetize end-user data. This is important because the internet of things allows many different objects and appliances to collect personal data. Fiduciary duties must also apply to smart homes, self-driving cars, and personal digital assistants.").

385 Balkin, *supra* note 59, at 11 ("[T]he law should treat digital companies that collect and use end user data according to fiduciary principles.").

386 *See* Israel Klein, *It's Time to Mind the GASB,* 54 SAN DIEGO L. REV. 565, 593 (2017) ("[I]t is impossible to provide information in any one report sufficient to meet the needs of all users.").

the relationship.[387] In our context, companies that operate delivery drones should neither "breach user trust" nor take actions that "users would reasonably consider unexpected or abusive."[388] As information fiduciaries, digital companies should avoid utilizing user data to manipulate users.[389]

Richards and Hartzog continued along this line, proposing that a comprehensive duty of loyalty should be imposed upon data collectors. Such trusted parties should subject their own interests to those made vulnerable through the extension of trust.[390] They suggest that data collectors should pursue the "best interests" of the trusting party with respect to that which has been exposed and entrusted.[391] Beyond personal data, individuals trust digital platforms "with their time, attention, experience, emotions, reputation, interpersonal relationships, vulnerabilities, and financial security."[392] Such platforms can influence user buying habits, emotions, and wellbeing and they should be loyal to their users. This is especially troubling as it has been empirically proven that there is an "automation bias" and people tend to trust algorithms more than they trust human advice.[393]

First, digital companies should avoid collecting and processing information, or mediating the digital environment, in a manner that conflicts with the best interest of their users (the trustees). Such a duty of loyalty can in fact dictate data minimization, limiting the purpose of data processing and usage, as well as refraining from direct marketing.[394] Another aspect of the duty of loyalty is to "invalidate waivers that attempt to relieve entrustees of obligations to avoid conflicted design or process" as a statutory prohibition on waiver.[395] A duty of loyalty can also impose requirements of disclosure and communication of important information to supersede cognitive biases such as information overload.[396] A determination that a breach of a duty of

---

387 Balkin, *supra* note 59, at 15.

388 *Id.* at 13; Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFF L. REV. 979, 1006–08 (2018); *see also* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1229 (2016); Michal Lavi, *Evil Nudges*, VAND. J. ENT. & TECH. L. 1, 68 (2018)

389 Lavi, *Evil Nudges*, *id.* (citing Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011, 2047-48 (2018)).

390 Richards & Hartzog, *supra* note 58, at 987.

391 *Id.* at 29.

392 Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U.L. REV. 961, 994 (2021).

393 Margot E. Kaminski & Jennifer M. Urban, *The Right to Consent AI*, 121 COLUM. L. REV. 1957, 1961 (2021); Nizan Geslevich Packin, *Consumer Finance and AI: The Death of Second Opinions?* 22 N.Y.U. J. LEGIS. & PUB. POL'Y 319, 344-46 (2020).

394 Richards & Hartzog, *supra* note 58, at 33.

395 *Id.* at 35.

396 *Id.* at 37.

loyalty constitutes a *per se* legal injury[397] would mitigate information privacy harm. It should be noted that beyond raising the awareness of users to practices of information collection and invasion, such disclosure might lead digital companies to change their behavior and reduce practices of invasion. Digital companies might do so and comply with disclosure duties because they are likely to overestimate the likely effect of disclosure on users, want to avoid shaming and preserve their reputation.[398]

A duty of loyalty goes further than procedural aspects of data protection regimes that are based on consent, which in effect give companies permission to engage in any manner of manipulation to extract information and fail to protect against opportunism. For example, restrictions of "purpose limitation" and "data minimization" can be diluted in practice through vague language and typically have exceptions for consent, that as explained, are rarely an effective limitation.[399] A duty of loyalty for data collectors can bridge the gap in information privacy protection, restricting manipulation by digital companies. Even though duties of loyalty are vague, like all legal standards, such as "negligence", they are expected to produce clarity over time. Furthermore, their vagueness can be an advantage, as it could allow flexibility that would in turn allow these duties to adapt to new innovative technologies, leaving policy makers and courts broad discretion, leading to optimal interpretation based on specific circumstances. Moreover, such a vague duty is likely to result in high standards of information privacy protection because when companies are not told exactly what they need to do to comply, they are likely to err on the side of caution.[400]

A duty of loyalty is not merely theoretical. Such duties are now a serious option for national privacy reform and have been included in pending privacy bills.[401] This concept can be expanded to fit an agenda, regardless of

---

397 *Id.* at 63.

398 *See* SUNSTEIN, *supra* note 171, at 108 ("Providers of information may well overestimate the likely effect of disclosure on consumers, partly because that disclosure seems so salient to providers.").

399 Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law, 99* WASH. U.L. REV. 961, 982 (2021).

400 *See id.* at 1013 ("When companies are not told exactly what they need to do to comply, they are likely to err on the side of caution. . . ."); *see also* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE 248-49 (2015) (explaining that ambiguity regarding the exposure to liability leads businesses to adopt higher standards relative to the standards that would have been adopted under clear rules).

401 *See* Richards & Hartzog, *supra* note 144 at 965 ("Leading federal privacy bills pending before Congress from both parties include proposed duties of loyalty, though they vary significantly in

whether a company bears specific obligations within specific relationships.[402] However, it seems that at this time the duty of loyalty should supplement affirmative duties of data protection,[403] as data can be collected in public, from people who have no relationship with the delivery service, and it is doubtful whether a duty of loyalty would apply in such context at this time.

After reviewing the EU data protection regime, the U.S. consumer protection approach, and proposals brought forward in emerging U.S. scholarship for a framework based on trust, the following Part of this Article presents conclusions regarding suggested guidelines for privacy and data protection in the context of delivery drones.

D. The Path Forward: Learning Lessons and Crafting a Framework for Regulating Delivery Drone Invasions of Privacy and Information Privacy Risks

Delivery drones collect information that is essential for improving delivery service. Drones can transmit information on weather, flight conditions and other parameters to an entire network of drones, thereby promoting efficiency. Furthermore, information collected by delivery drones can advance the platform's business model and promote innovation. However, there should be safeguards to secure privacy.

Today, in the face of advanced technology, privacy can be violated even in public spaces. It is unrealistic to base privacy models on consent, since individuals in these public spaces lack contractual relations with the drone operators. Moreover, even where the injured party is the person who ordered the delivery and contractual relations do exist, it is almost impossible to gain meaningful consent.[404] Therefore, the law should neglect principles

---

scope, specificity, and justification.") *see e.g.*, Data Care Act of 2019, S. 2961, 116th Cong. § 2 (2019) ("Duty of Loyalty: An online service provider may not use individual identifying data, or data derived from individual identifying data, in any way that—(A) will benefit the online service provider to the detriment of an end user; and (B) (i) will result in reasonably foreseeable and material physical or financial harm to an end user; or (ii) would be unexpected and highly offensive to a reasonable end user.").

402 *See* Richards & Hartzog, *supra* 144 note at 1010 ("This would mean crating rules and frameworks designed to prospectively encourage fidelity prescriptively and to discourage opportunistic behavior regardless of whether a company owes specific obligations within specific relationships.").

403 *See id.* at 1017 ("[W]e are not advocating for a duty of loyalty in privacy law *in place* of a robust data protection regime. We are arguing for a duty of loyalty *in addition* to it . . . . So, while loyalty might only apply within the confines of a relationship, data protection rules apply to everyone that touches the data.").

404 *See* Citron & Solove, *supra* note 156 at 52 ("When people use an app that thwarts their privacy expectations, people's ability to assess the risks of using the app is impeded. The market cannot work fairly if people's expectations are completely wrong, if people lack knowledge of potential

of reasonable expectation of privacy and consent, and shift the privacy framework to affirmative prohibitions and supplemental standards that would reduce the intrusive activities allowed by technology.

The suggested framework proposed by this Article includes the following principles:

Principle I: Avoid peering into private homes, maintain distance from private buildings, avoid documenting the home of the person who ordered the delivery

This principle preserves the traditional privacy rationale of "the right to be let alone" and the prohibitions against peering and intruding upon seclusion.[405] Precisely because the dichotomy between private and public spaces collapses, the context of home becomes more sensitive. The potential for infringement of personal autonomy by a drone peering into a private home is great. Information privacy violations in the home can be particularly grave because the home houses a plethora of potentially personal information. Such sensitive information can provide drone operation companies with conclusions about the consumer's lifestyle and make it easy for them to manipulate consumers. Finally, eliminating peering into private homes in such cases could also mitigate security risks in case of a data breach of the delivery drone database by criminals, which could end in a brick-and-mortar invasion into the house of the person who ordered the delivery, thereby reducing the likelihood of burglary or theft.

In order to protect privacy at home, delivery drones should refrain from peering into homes and maintain a distance, as far as possible from private property.[406] Yet, when drones deliver parcels, they must fly close to the consumer's house. In addition, due to the FAA line of sight requirement,[407] drones cannot always keep their distance. To mitigate invasion of privacy, drones should avoid taking any pictures or documenting the consumer's home. Regulations can impose limitations on the flying path in order to reduce flying over third party property where possible.

---

future uses of their personal data, and if people have no way to balance the benefits and risks of using products or services."); *see also* Richards & Hartzog, *supra* note 144, at 1486 (referring to three pathologies of consent and defining *coerced consent* as "a choice that takes the 'voluntary' out of 'knowing and voluntary'"). For example, during COVID-19 lockdowns, one of the only options to get meals was by using Wolt for food delivery, as the restaurants were closed for T.A.

405 *See supra* Part II (A) ("Civil Law: Privacy Torts")

406 *See supra* note 356. This principle adopts the recommendation of "Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilization of Drones."

407 *See supra* note 25, and the text attached to it.

Principle II: Privacy–by–design: Obscuring information in public spaces and minimization of collection

Delivery drones collect information in public spaces. This information allows the platforms that operate them to improve their delivery service as well as the platform user's experience. For example, it allows the platform to map the drone's path, identify the location of the closest drones in the network, better distribute the delivery load, and increase efficiency. Such information can even improve the consumer's experience using the platform, by learning about the consumer's general needs. For example, information about what people are wearing or the local weather, can be helpful in providing consumers with product recommendations that fit the general needs of people living in the same area. However, as explained above, in the past, information about individuals in public remained obscured, but digital technologies have changed that. High-resolution cameras and facial recognition technologies make it possible to identify specific people in public, gain specific behavioral insights on them, profile them, and draw conclusions about them.[408] Such insights can be gained even about individuals who are not using the delivery service. Even though such invasions of privacy are technologically possible they should not take place.

In order to mitigate invasions of privacy in public while avoiding hindering innovation and development of drone delivery services, service operators should build privacy friendly systems, starting at the stage of drone design. They should implement measures to protect the privacy of identifiable individuals. To do so, drone operators should collect *only the information needed to improve the service*. Alternatively, they can ex ante *avoid high-resolution* cameras and facial recognition technology,[409] in fact, such an idea is reflected in the EU's recent proposed regulation regarding the use of AI. This regulation proposes to ban real time remote biometric identification in public places.[410] In fact, other jurisdictions are also concerned with this issue

408 KATE CRAWFORD: ATLAS OF AI 154 (2021).

409 FRANK PASQUALE, NEW LAWS OF ROBOTICS: DEFENDING HUMAN EXPERTISE IN THE AGE OF AI 127 (2020) ("Limiting of facial recognition technology ensures that at least some freedom to move anonymously, with one's whereabouts and identity unmonitored by prying eyes.").

410 *Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, at Art. 5(1)(a)-(d) COM (2021) 206 final (Apr. 21, 2021); For further information, see Thomas Burri & Fredrik von Bothmer, The New EU Legislation on Artificial Intelligence: A Primer, (Apr. 21, 2021) (unpublished manuscript) (manuscript at 2), https://ssrn.com/abstract=3831424; Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, 22 COMPUT. L. REV. INT'L (forthcoming), https://arxiv.org/ftp/arxiv/papers/2107/2107.03721.pdf [https ://perma.cc/W5NB-GKBK].

and have offered similar regulatory solutions. Regulators in Australia recently banned limitless scrapping for facial recognition.[411] In addition, some corporations have voted for self-regulating in this area, the prime example being Facebook which has recently announced that due to the ambiguity, it will shut down its facial recognition system.[412] Another possibility is to implement technology *to blur faces,* or other identifying information on individuals ex post by using technology. Such technology is already available today and was used by Google-Street in response to privacy concerns that private information might appear on public maps.[413] Such obscurity by design is the preferable way to protect privacy,[414] especially in public. It allows degrees of privacy and is superior to an all or nothing approach. It may also enhance safety by reducing the harm if a data breach to the drone, or the platform occurs.[415] Indeed, blurring technology that in fact anonymizes identifying information can be de-anonymized by companies that operate delivery drones, by data brokers that might purchase information, and even by hackers in cases of data breach to the database of the drone or the platform operating it. However, such blurring technology minimizes re-identification risks and reduces the likelihood of violation of privacy of individuals in public.[416]

Principle III: Data Retention Limitation

Delivery drones are engaged in surveillance capitalism. Collecting, analyzing and retaining information are the base for extensive influence and manipulation. For example, information collected by drones, combined with personal information collected by the platform that operates them online, can be used for personalization, and might limit consumers' opportunities, based on past behavior and activities. Influencing consumer decision-making by utilizing data driven models might shape future behavior, choices,

411 Mack DeGeurin, *Clearview AI Forced to Cease Data Scraping Operations in Australia*, GIZMODO (Nov. 3, 2021) https://gizmodo.com/clearview-ai-forced-to-cease-data-scraping-operations-i-1847991895 [https://perma.cc/9XUT-6J43].

412 Sheila Dang and Elizabeth Culliford, *Facebook Will Shut Down Facial Recognition System*, REUTERS (Nov. 3, 2021) https://www.reuters.com/technology/facebook-will-shut-down-facial-recognition-system-2021-11-02/ [https://perma.cc/3SX5-D356].

413 *See* Stephen Shankland, *Google Begins Blurring Faces in Street View*, CNET (May 13, 2008), cnet.co/38xeAcF [https://perma.cc/M7YD-4DXL]; *see also* Patrick Gallo & Houssain Kettani, *On Privacy Issues With Google Street View*, 65 S.D. L. REV. 608, 608-13 (2020).

414 Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 752 (2016).

415 Michael Froomkin & Zak Colangelo, *Privacy as Safety*, 95 WASH. L. REV. 141, 155 (2020).

416 *See* Rubinstein & Hartzog, *supra* note 375, at 703 (arguing that anonymization should focus on the process of minimizing risk of reidentification and sensitive attribute disclosure, not preventing harm).

and desires, as algorithms adapt themselves according to past activities.[417] Instead of focusing on the stage of influence itself, it is proposed to limit the duration of retention of personal data.[418] Such a principle has the potential to mitigate the depth of the platform's influence on consumers. It can mitigate the problem of tying individuals to their past transactions. Thus, by default, identifiable personal data should be deleted. Limitations on the duration of data retention are likely to mitigate the possible harm of manipulation. The less data companies collect and store, the less they can influence choice.[419] In addition, it is advisable to allow people to request that companies maintaining their data delete the data even prior to the end of the personal data retention limit. This suggestion learns a lesson from the "right to erasure" in the EU regulation.[420]

Principle IV: Transparency and impact assessment as safeguards

Delivery drone operators should be transparent about the technologies they implement and their capacity to invade privacy. They should also be transparent about the information they collect, and their algorithmic analysis of information in the short term, before data is deleted.[421] Yet, algorithmic analysis is opaque and difficult to challenge.[422] One must bear in mind that algorithms are regarded as trade secrets. Moreover, most individuals without specialized knowledge are likely to find disclosure regarding the function of algorithms useless.[423] Therefore, it is proposed that algorithmic impact assessment should be conducted.[424] Accordingly, platform operators would

---

417 *See* ZUBOFF, *supra* note 50at 329-45 (explaining that this is an infringement on what she defines "right to future tense").

418 Tsesis, *supra* note 111.

419 *See* SINAN ARAL: THE HYPE MACHINE: HOW SOCIAL MEDIA DISRUPTS OUR ELECTIONS, OUR ECONOMY, AND OUR HEALTH AND HOW WE MUST ADAPT 207 (2020) (conducting an experiment and discovering that advertisement campaigns were 65 percent less efficient when laws restricting data access for microtargeting were implemented).

420 GDPR, *supra* note 56, at art. 17.

421 Scott, *supra* note 232.

422 *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 8-9 (2015) (explaining that the judgment of software is secret and operates under laws of secrecy and technologies of obfuscation, creating a "black box" that is difficult to challenge).

423 *See* Ari Ezra Waldman, *Power, Process, and Automated Decision-Making*, 88 FORDHAM L REV. 613, 628-29 (2019) (noting that transparency around algorithms is "functionally unhelpful" to those who do not have specialized knowledge about source code).

424 *See id.* at 628-29 ("Algorithmic impact assessments can identify and evaluate risks, consider alternatives, identify strategies to mitigate risks, and help articulate the rationale for the automated system . . . ."). *See also* Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection,* 61 B.C. L. REV. 1687, 1758-59 (2020) (referring to algorithmic impact assessment

have to ascertain that their algorithms and tools undergo regular evaluation for safety by independent auditors and technology experts. Algorithmic impact assessments could mitigate the risk for error or failure at the design stage, or unexpected reactions of learning algorithms that might result in unlawful influences.

This idea is not so revolutionary: the need to evaluate algorithms is reflected in recently proposed regulation in the EU, regarding Artificial Intelligence.[425] Recently, in the U.S., legislators proposed to apply impact assessments in the context of discrimination. A bill entitled "Algorithmic Accountability Act of 2019"[426] requires entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments to mitigate discrimination, and work to correct them in a timely manner. Such a proposal can be applicable for safeguarding violations of information privacy by platforms that operate delivery drones.

A Meta-Standard: Loyalty Duties Beyond Privacy and Data Protection

A meta-standard of the framework is adopting scholars' proposals[427] to understand privacy in terms of trust between users and platforms and accordingly impose a duty of loyalty on data collectors. Such a flexible open standard would apply primarily to information about drone delivery service users. However, over time this standard could be expanded to a more extensive norm. Accordingly, platforms that collect information on their users should pursue the "best interests" of the trusting party with respect to

---

for "high-risk automated decision systems"); Deirdre K. Mulligan & Kenneth A. Bamberger, *Procurement as Policy: Administrative Process for Machine Learning*, 34 BERKELEY TECH. L.J. 773, 832 (2019). ("The recently introduced Algorithmic Accountability Act of 2019 . . . requiring automated decision-system, data protection impact assessments, and regulations promulgated by the Federal Trade Commission to guide such assessments"); Margot E. Kaminski & Gianclaudio Malgieri, *Algorithmic Impact Assessments Under the GDPR: Producing Multi-Layered Explanations*, 11 INT'L DATA PRIV. L. 125, 130 (2021) Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 114 (2019) ("In Europe, the GDPR and Police and Criminal Justice Authorities require data protection impact assessments (DPIA) whenever data processing "is likely to result in a high risk to the rights and freedoms of natural persons.").

425 *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21 2021); Michal Lavi, *Targeting Exceptions*, 32 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 65, 157, 161(2021); Margot E. Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. (forthcoming 2023) (at 49–54), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195066 [https://perma.cc/C9NDXJN].

426 *See* Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019) (directing the "Federal Trade Commission to require entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments").

427 *See supra* Part III, in particular *supra* notes 376-377 and the text attached to them.

what is exposed and entrusted. This open standard is expected to mitigate data collection, processing or mediating information of drone delivery service users against their best interest. Such a framework could encompass the principles of the EU regulation regarding data minimization and purpose limitation. Beyond this, the flexibility provided by a duty of loyalty does not focus on a specific marketing strategy such as personalized advertisements. Thus, in contrast to concrete rules, a duty of loyalty can be adapted and interpreted to mitigate all types of undue influence.

A duty of loyalty is about trust between data collectors and their trustees, therefore the duty would not apply to third parties that might purchase personal data from platforms, such as data brokers. However, because a duty of loyalty is about acting in the best interest of the trusting party, the duty is likely to restrict the platforms from transferring user data to third parties for commercial purposes in the first place, if transferring such data would be contrary to the self-interest of users.

Such a framework could allow individual rights of action in court as it is based mainly on relations between parties, and it could provide remedies to delivery drone service users. A breach of a duty of loyalty would be a *per se* legal injury that could solve the standing problem that requires concrete legal injury.[428] The injury caused by a breach of the duty of loyalty is the harm to the trust in the relationship rather than a pecuniary or emotional injury. Thus, loyalty litigation would have real advantages over tort claims that focus on tangible consequences of privacy invasions.[429]

In summary, the proposed framework that includes concrete principles and an open meta-standard of duty of loyalty makes it possible to clarify grey areas and insert values to information privacy, and therefore it is promising. This framework expands individual data rights, and mitigates information privacy harm that can be inflicted by delivery drones. It is proposed that the federal government should set at least minimum national rules according to the principles proposed, while the states can experiment with legislative rules beyond the minimum.[430]

---

428 *See* Neil Richards & Woodrow Hartzog, *Legislating Data Loyalty*, 97 NOTRE DAME L. REV. REFLECTION 365, 371 (2022); Richards & Hartzog, *supra* note 58, at 51 (referring to the jurisdictional requirements of Article III standing). *See also* Spokeo, Inc. v. Robins, 578 U.S. 330, 334 (2016) (emphasizing that an injury must be concrete and particularized to satisfy standing).

429 *See* Richards & Hartzog, *supra* note 58, at 51 (noting that plaintiffs that have "'intangible' injuries like privacy claims must now as a constitutional matter show the additional requirement of the 'concrete' injury in fact").

430 *See* Kaminski, *supra* note 105, at 74 (arguing that Congress should not preempt states from enacting privacy laws for civilian use of drones, but should instead let States experiment with regulation first).

IV. ADDRESSING FIRST AMENDMENT CONCERNS

Regulating drone delivery services to protect privacy may limit freedom of speech and collide with First Amendment protection.[431] This Part addresses such constitutional concerns. Unlike the EU, which balances between free speech, privacy and data protection, in the U.S. restrictions on speech are limited to narrowly confined categories.[432] The First Amendment protects freedom of speech, including "expressive activity (speech mixed with action)," and activities necessary for speech, limiting the government's ability to restrict free speech.[433] As a result, in the U.S. many types of privacy protections can easily be attacked as unconstitutional.[434]

Limitations on privacy protection of the distribution of information have been set down in a series of First Amendment cases. Recent years have witnessed a shift in free speech priorities beyond the protection of political speech, expanding it to include commercial speech and protecting corporations,[435] among them companies that operate delivery drones. Courts have protected a "right to record" and have even applied the First Amendment to collection of raw data.[436] In *Sorrell*, a Vermont statute prohibited data mining of pharmaceutical prescription files and restricted the sale, disclosure and use of records containing information about physician prescribing practices.[437] Pharmaceutical companies used this data to

---

431 *See* U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech, or of the press.").

432 *See, e.g.*, United States v. Alvarez, 567 U.S. 709, 717 (2012) (describing categories of speech that have restrictions, such as obscenity and defamation); Michal Lavi, *Do Platforms Kill?* 43 HARV. J.L. & PUB. POL'Y 477, 534 (2020) (noting that terrorist content, such as "solicitations to commit crimes," is not protected speech under the First Amendment); Richards & Hartzog, *supra* note 298, at 1730 ("[I]n the United States, the fundamental right of free expression protected by the First Amendment is not subject to proportionality analysis—if a court finds that there is a First Amendment right, then the First Amendment applies to the state action, and strict scrutiny normally applies.").

433 *See* Chander et al., *supra* note 300, at 53-54 (noting that the First Amendment may pose constraints on drafting privacy laws due to its protections of free speech).

434 *See* Richards & Hartzog, *supra* note 298, at 1727 (noting that in the U.S. there are implicit constitutional protections for privacy against the government in the First, Third, Fourth, Fifth, and Fourteenth Amendments).

435 For criticism, see MARY ANNE FRANKS, THE CULT OF THE CONSTITUTION, 13, 117-23 (2019) (arguing that legislators, courts and civil rights organizations have interpreted the First Amendment selectively, almost like religious fundamentalists, and in fact they have infringed on the right of minorities and less powerful populations to free speech, shifting even more power from vulnerable populations to powerful ones).

436 *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 557 (2011) (finding First Amendment protection for "speech in aid of pharmaceutical marketing").

437 *Id.*

convince physicians to prescribe expensive medications.[438] The Supreme Court struck down the law on First Amendment grounds, holding that these restrictions warranted heightened judicial scrutiny.[439] Such expansive First Amendment protections can make the application of privacy regulation, and the proposed framework in particular, quite complex, and there might be a risk that courts will struck it down as unconstitutional.[440] However, it would seem that "If 'data' were somehow 'speech,' and this had First Amendment consequences, constitutional doubt would cloud virtually every form of economic regulation we have."[441]

Clearview AI, a facial recognition technology company, recently downloaded billions of photos from the Internet and analyzed biometric information from the images in the database. This made it possible for users to upload a photo of any person and immediately view all publicly available photos of that person, along with links to where those photos appear. A class action was filed seeking an injunction to limit the company from collecting and retaining such information.[442] Clearview AI plans to argue a free-speech right to dissemination of photos,[443] and claim that Illinois' Biometric Information Privacy Act (BIPA),[444] which would prohibit such dissemination, violates the First Amendment and is unconstitutional. If Clearview AI's

---

438 *See* Tamara R. Piety, *A Necessary Cost of Freedom - The Incoherence of Sorrell v. IMS*, 64 ALA. L. REV. 1, 6 (2012). ("Data mining is one of many tools pharmaceutical companies use to market brand-name drugs. Because heavier use of brand-name drugs over generics raises the cost of health care, Vermont wanted to regulate this practice.").

439 *See id. See also* Jane R. Bambauer & Derek E. Bambauer, *Information Libertarianism*, 105 CALIF. L. REV. 335, 361 (2017) (discussing the Supreme Court's decision in *Sorrell v. IMS Health Inc.* to strike down a Vermont statute "as a content-based restriction of speech that failed to meet strict scrutiny").

440 *See* Kaminski, *supra* note 105, at 60-64 (discussing First Amendment and privacy concerns that may arise if the federal government implements regulations for civilian drone usage).

441 Neil M. Richards, *Why Data Privacy Law Is (Mostly) Constitutional*, 56 WM. & MARY L. REV. 1501, 1507 (2015).

442 Complaint, David Mutnick v. Clearview AI, Inc., No 1:2020cv00512 (N.D. Ill. Jan. 22, 2020) .

443 *See* Kashmir Hill, *Facial Recognition Start-Up Mounts a First Amendment Defense*, N.Y. TIMES: TECH., https://www.nytimes.com/2020/08/11/technology/clearview-floyd-abrams.html [https://perma.cc/RDD4-CGRB] (Aug. 11, 2020) (discussing Floyd Abrams' plan to argue that Clearview AI's sale of access to a database of photos downloaded from the Internet is a form of free speech).

444 Biometric Information Privacy Act, 740 ILL. COMP. STAT. § 14/5 (2008) (enacting a law that aims to regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information); Michelle Jackson, *Opting Out: Biometric Information Privacy and Standing*, 18 DUKE L. & TECH. REV. 293 295, 301 (2020).

argument succeeds, such a precedent could undermine America's privacy protection.[445]

Scholars broadly disagree on how much of privacy law survives First Amendment challenges.[446] On one side of the spectrum, it has been argued that First Amendment protection is far-reaching, protecting even raw data as it promotes the creation of knowledge.[447] On the other side of the spectrum, privacy scholars have argued that just because something is speech does not mean it is beyond regulation. The value of speech is not absolute and arguments that "data is speech" collapse under serious analysis.[448] Furthermore, scholars have argued that lack of privacy can hinder free expression, as privacy is necessary in order to produce speech.[449] Therefore, they have argued that privacy laws do not infringe on free speech but rather promote it.

Recently, Professor Jack Balkin defended most privacy regulation and argued that it is consistent with the First Amendment.[450] Focusing on fiduciary duties under the framework of trust, he explained that such duties limit information disclosure in ways that undermine the interests of the beneficiaries of the data collection. As disclosure occurs in the context of a

---

445 *See* Woodrow Hartzog & Neil Richards, *Getting the First Amendment Wrong*, BOS. GLOBE, (Sept. 4, 2020, 3:03 AM), https://www.bostonglobe.com/2020/09/04/opinion/getting-first-amendment-wrong/ [https://perma.cc/P6CQ-4M6M] (arguing that privacy protections would be eviscerated if Clearview AI successfully asserts a "free speech right to disseminate publicly available photos" because Americans would no longer be able to sue companies directly for violations of the First Amendment).

446 *See, e.g.*, Chander et al., *supra* note 300, at 54 (noting that "[c]ommentators broadly disagree on how much of data privacy law might survive First Amendment challenges").

447 *See generally* Jane Bambauer, *Is Data Speech?* 66 STAN. L REV. 57, 60-61 (2014) (explaining that the First Amendment can protect raw data as it promotes the creation of knowledge).

448 *See* Richards, *supra* note 441, at 1524 (criticizing that the "data-is-speech" argument and noting that "[j]ust because something is speech does not mean it is beyond regulation"). *See also* Richards & Hartzog, *supra* note 298, at 1731 ("Arguments that 'data is speech' and thus data protection rules are censorship have rhetorical appeal, even though they break down completely under serious analysis."); Lavi, *supra* note 183, at 2644-45 (arguing that the First Amendment and the "right to be forgotten" can co-exist and arguing that "the value of speech is not absolute. With time, data may express fewer elements of free speech . . . . nuanced protection of speech should be promulgated. It should take into account the time that had passed from publishing the original expression to the present").

449 *See* NEIL RICHARDS, INTELLECTUAL PRIVACY–RETHINKING DIGITAL LIBERTIES IN THE DIGITAL AGE 11, 109-136 (2015) (referring to Freedom of thought, the right to read freely and the right to communicate in confidence). *See also* PASQUALE, *supra* note 409, at 127 ("The great irony here is that the corporate assertion of constitutional rights creates databases that will have enormous chilling effects on ordinary citizens' speech.").

450 Balkin, *supra* note 59, at 29-31 (arguing that the "fiduciary model explains why many privacy regulations are consistent with the First Amendment").

confidential relationship, regulation is needed to protect users from manipulation. In such cases, regulation aims at different stages of the information cycle.[451] The First Amendment interacts differently with different types of privacy regulation. Regulation of collection of information raises less First Amendment concerns because it aims at conduct,[452] which is not inherently expressive, as opposed to speech. Even if general collection of information can be considered speech, it is content neutral, limiting expression without regard to the content or communicative impact of the message conveyed. Thus, it is subject only to the intermediate scrutiny test.[453] As privacy regulation is an important privacy interest and regulation is substantially related to that interest, it would pass the test. Regarding disclosure, distribution and sale of information: "the First Amendment properly distinguishes between information obtained in the course of fiduciary relationships—which states can usually protect from disclosure — and information obtained in other contexts."[454] Regulating distribution of data in the course of a user-platform relationship could thus be in line with the First Amendment.

Under such a reading of the First Amendment, the proposed Framework would survive First Amendment scrutiny. Regarding **principle I**–limitation on peering–this is a content neutral limitation, and as such it is not subject to the strict scrutiny test. Since privacy interests are important and the regulation is substantially related to those interests, it would past the intermediate scrutiny test. Regarding **principle II**–minimization and obscuring–the framework does not restrict data collection altogether. It prefers a "privacy by design" approach, allowing the obscuring of information using anonymization tools. Therefore, it does not conflict directly with the First Amendment. Obscuring and anonymization could even prevent chilling user and third-party speech: if they know the data

451 *See id.* at 30 (referring to regulations about "(1) collection of information, (2) collation, (3) analysis, (4) use, (5) disclosure and disattribution, (6) sale, and (7) retention or destruction").

452 *Cf.* United States v. O'Brien, 391 U.S. 367, 375-76 (1968) (articulating the distinction between speech and conduct).

453 *See* Balkin, *supra* note 59, at 30-31 (noting that "[t]he First Amendment interacts differently with these different kinds of privacy regulations"). *See* Shaun B. Spencer, *Two First Amendment Futures: Consumer Privacy Law and the Deregulatory First Amendment*, 2020 MICH. ST. L. REV. 897, 911, 922 (2020). ("In contrast, content-neutral laws trigger only intermediate scrutiny."); Katja Kukielski, *The First Amendment and Facial Recognition Technology*, 55 LOY. L.A. L. REV. 231, 238-39 (2022). ("[W]hen companies sell FRT data for purposes that do not contribute meaningfully to the purposes behind the First Amendment, regulation on such disclosures should be subject only to some form of intermediate scrutiny.") *Id.* at 257. ("[L]aws regulating the collection of faceprints are content- and viewpoint-neutral and should therefore receive some level of intermediate scrutiny.").

454 Balkin, *supra* note 59, at 30.

collected on them is anonymized, they are more likely to engage freely in public expression, including free speech. Regarding **principle III**–data retention–even if data is considered speech, over time data may take on fewer characteristics of free speech.[455] Moreover, the marketplace of commerce is not the marketplace of ideas. Commercial collection and analysis of data is not public opinion but rather a form of market behavior that uses speech.[456] Furthermore, commercial entities do not have any constitutional right to retain data indefinitely. Therefore, regulation limiting data retention should be subject to intermediate scrutiny standards. Regarding **principle IV**–transparency and impact assessment–there is no conflict with the First Amendment and no speech censorship. Quite the contrary, this principle is likely to promote freedom of expression as such obligations promote the public right to receive information, which is part the marketplace of ideas rationale.[457]

The meta principle of duty of loyalty would restrict data-driven manipulation when data was obtained in the course of a fiduciary relationship. Limitations on data-distribution, even using targeted ads, can therefore withstand First Amendment scrutiny. Furthermore, even if overbroad restrictions on manipulation were to encounter difficulty on constitutional grounds, the worst of such manipulative practices could be curtailed by principle III: limitations on data retention. If less data is retained, targeted ads based on data collection would be limited in scope and their ability to manipulate consumers would be minimized. This type of regulation would not only decrease the vulnerability of consumer decision-making to commercial offers that seek to take advantage of consumer weaknesses and opportune timing, it might even have a beneficial impact on consumer standing within future commercial offers and opportunities. [458]

To conclude, even though scholars disagree on the scope of First Amendment protection, we believe that most of the principles of the

---

455 *See* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 147–63 (2016) (arguing that data can be considered speech, but the scope of the First Amendment with regard to protecting data is not absolute). *Cf.* Tsesis, *supra* note 111, at 1626 ("In an age of such immense private data retention, the U.S. should join Europe by adding consumer privacy regulations of the internet to better preserve natural persons' fundamental rights to dignity, autonomy, and privacy.").

456 Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics,* MD. L. REV. 439, 502 (2020).

457 Richards & Hartzog, *supra* note 298, at 58; On listeners' right to access information, see Tsesis *supra* note 111, at 599.

458 On manipulation of opportunities in the context of discrimination, see Pauline T. Kim, *Manipulating Opportunity*, VA. L. REV. 867 (2020) (arguing that less available information has the potential to reduce discrimination).

proposed framework can withstand First Amendment scrutiny. Even if the concept of trust in relations and duty of loyalty poses more First Amendment challenges, principle III which focuses on data retention limitation, can narrow the gap and limit the scope and depth of manipulation based on data driven models which become more invasive due to delivery drone capabilities.

CONCLUSION

Someday soon, you may not wait for packages to arrive by truck–instead, they'll come overhead, via drone. Delivery drones have truly disruptive potential in the field of deliveries, and they can be a game changer in the industry of delivery services due to the groundbreaking benefits they offer.[459] Yet, there is a flip side, since delivery drones also possess groundbreaking surveillance capabilities. These "eyes in the sky" are designed to follow individuals wherever they go, equipped with high-resolution cameras, recording systems and sensors. This technology can collect information on individuals in private and in public. The information collected can be utilized for data driven models of commerce, influencing consumer decision-making and future consumer commercial opportunities, through manipulation. Delivery drones give rise to pervasive surveillance and raise new challenges to privacy policy makers.

This Article mapped out the types of privacy violations and privacy challenges posed by delivery drones. Next, it argued that the existing basic parameters for establishing violation of privacy–reasonable expectation and consent–are ill-equipped to address privacy challenges in the age of surveillance capitalism. It explained that the dichotomy between private and public collapses in the face of new technology and that negative theories of privacy such as the "right to be let alone" fail to address potential harm to information privacy harm resulting from the influence of platforms that operate delivery drones on consumer decision making through data driven models. This Article proposed a framework for regulating delivery drones that includes rules and a meta standard of protecting trust between delivery drone service users and the companies that operate the drones. Finally, it addressed First Amendment concerns regarding the proposed framework.

---

459 *See* Ian Sherr, *UPS, Amazon Delivery Drones a Step Closer to Reality with New US Rules*, CNET (Dec. 29, 2020, 11:07 AM), https://www.cnet.com/news/ups-amazon-delivery-drones-a-step-closer-to-reality-with-new-us-rules/ [https://perma.cc/U99F-RXJF] (discussing the FAA's adoption of new regulations for drones that brings the US closer to having delivery of packages by drones).

The proposed framework has vast potential to meet the privacy challenges posed by delivery drones, to ensure that the use of delivery drones does not bring about the demise of privacy. This Article therefore concludes with a call for policy makers, federal and state legislators, to adopt the proposed framework.