

Journal of Technology Law & Policy

Volume 23

Number 2

ARTICLES

LOOK! IT'S A BIRD! IT'S A PLANE! NO, IT'S A
TRESPASSING DRONE *Nanci K. Carr* 147

WE NEED TO TALK ABOUT DATA: HOW DIGITAL
MONOPOLIES ARISE AND WHY THEY
HAVE POWER AND INFLUENCE *Daniel McIntosh* 185

NOTES

THE PSYCHOLOGICAL AND VIRTUAL SIEGE OF
LOOT BOXES *Elpidio K. Cruz* 215

A NEW AGE OF AUTHENTICATION *Abraham Oxner* 229

EDITORIAL BOARD

2018–2019

EDITOR IN CHIEF
Rebekah Allison

ASSISTANT EDITORS IN CHIEF
Aaron Crews
Brendan Collins

EXECUTIVE EDITOR IN RESIDENCE
Adam J. Duso

EXECUTIVE MANAGING EDITOR
Ashley Genoese

EXECUTIVE ARTICLES EDITOR
Justin Shifrin

EXECUTIVE STUDENT WORKS EDITOR
Ellyse Collins

EXECUTIVE RESEARCH EDITOR
Shannon Anderson

EXECUTIVE GALLEYS EDITOR
Michael Liles

EXECUTIVE COMMUNICATIONS EDITOR
Patrick Salmon

GENERAL BOARD

2018–2019

Farhaan Anjum
Andrew Bayudan
Avigail Bacharach
Alexandra Beguiristain
Tyra Carroll
Jacob Cohen
Elpidio Cruz
Melissa Dangond
James Dority
Jacob Duval
Kimano Edwards
Michael Farhat
William Ford
Michael Friedman
Mendel Harlig
John Harper
Laura Hendee
Geneva Hernandez
Matthew Hutchisson
Andrew Ingber
Ian Johnson
Jessey Krehl

Brett Lashley
Carlos Lievano
Gabriella Morillo
Abraham Oxner
Esther Oyetoro
Gabriel Pla
Stephanie Pocatko
Jacob Post
Ty Pryor
Richard Russo
John Rutledge
Eleanor Samuels
Alfredo Sarduy
Matthew Sawyer
Michael Shepherd
Justin Shifrin
Brandon Singh
Lana Smith
Mariya Solomiy
Bradley Spivey
Kyle Swanson
Luke Tobis
Richard Windisch

FACULTY ADVISOR
Stacey Steinberg

STAFF EDITOR
Lisa Caldwell

LOOK! IT’S A BIRD! IT’S A PLANE! NO, IT’S A TRESPASSING DRONE

Nanci K. Carr*

Abstract

Drones have become increasingly popular as new uses are continuously discovered. However, landowners who watch drones fly over their yards and peer into their windows may not be as excited as the drone enthusiasts. Landowners are asking, “How can I keep that drone away from my property?” Do existing property laws addressing trespass and nuisance sufficiently protect landowners from unwanted drones? What rights and remedies are available to landowners to curtail intrusive drone use? How can business owners secure their property to prevent drones from obtaining confidential information during a drone flight? And how do state and federal regulators manage the challenges of navigation, hardware reliability, and airspace management?

INTRODUCTION	148
I. WHAT ARE DRONES AND HOW ARE THEY USED?.....	150
A. <i>What Are Drones?</i>	150
B. <i>How Are Drones Used?</i>	151
II. AIRSPACE RIGHTS.....	156
A. <i>Trespass</i>	156
B. <i>History of Airspace Rights</i>	156
C. <i>FAA Regulation of Airspace</i>	158
D. <i>Integration of UAVs into the United States Airspace</i>	160
E. <i>Penalties for Unregistered Drones</i>	163
F. <i>Line of Sight Restrictions</i>	164
III. AIRSPACE TRESPASS.....	167
A. <i>Airspace Trespass by Something Other than Drones</i>	167
B. <i>Airspace Trespass by Drones</i>	171
IV. STATE AND LOCAL REGULATION OF DRONES.....	172
A. <i>State Regulation of Drones</i>	172
B. <i>Local Regulation</i>	176
1. Community Regulation	176
2. Prevention of Drones.....	177
3. University Regulation	178

* Nanci K. Carr, Assistant Professor of Business Law at California State University, Northridge. J.D., *cum laude*, Southwestern Law School; B.S., Business Administration, Ball State University. This Article benefitted from valuable feedback at the Huber Hurst Seminar at the University of Florida. Thanks to my research assistant, Steven Kyle Waldrop, CSUN Class of 2019, and the CSUN Real Estate Center for funding support.

V.	ADDITIONAL TORTS.....	178
	A. <i>Nuisance</i>	178
	B. <i>Invasion of Privacy</i>	180
VI.	FUTURE FOR DRONE OPERATORS	180
	CONCLUSION.....	182

INTRODUCTION

Remotely piloted aircraft known as “drones” are becoming increasingly popular with both individuals and businesses, and new uses are discovered daily. In fact, the Federal Aviation Administration (FAA) anticipates that by 2021, the number of recreational drones in use could reach as high as 2.94 million and that commercial drones could reach over 600,000.¹ Hobbyists fly drones for fun on a Sunday afternoon, businesses use them to deliver goods, and law enforcement officers use them to conduct searches with less personal risk to officers.² They are even being tested as a taxi service, with the hope of transporting people.³ However, landowners who are watching drones fly over their yards and peer into their windows may not be as excited as the drone users. Sixty-three percent of respondents to a recent Pew Research Center survey felt “it would be a change for the worse if *personal and commercial drones are*

1. FED. AVIATION ADMIN., FAA AEROSPACE FORECAST: FISCAL YEARS 2018–2038 41, 43 (2018), https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2018-38_FAA_Aerospace_Forecast.pdf.

2. The use of drones for warrantless searches is subject to well-established search and seizure precedents under the Fourth Amendment. *See* *United States v. Jones*, 565 U.S. 400, 404 (2012) (holding that the attachment of a GPS tracking device to a vehicle and use of that device to monitor a vehicle’s movement on public streets constitutes a trespass and therefore a search under the Fourth Amendment); *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding that the use of sense-enhancing technology, or thermal imaging, to gather information regarding the interior of a home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search requiring a warrant); *Florida v. Riley*, 488 U.S. 445, 455 (1989) (holding that a warrantless aerial observation of the interior of a partially covered greenhouse in a residential backyard from a helicopter flying at 400 feet was not unreasonable under the Fourth Amendment); *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (holding that a warrantless aerial observation of fenced-in backyard from an aircraft flying at 1,000 feet was not unreasonable under the Fourth Amendment).

3. In Dubai, a 2-seat unmanned vehicle designed by German firm Volocopter, took off for a five-minute flight, watched by Crown Prince Sheikh Hamdan bin Mohammed. Volocopter hopes to have unmanned taxis ready for commercial use within five years, and Dubai, wanting to be the “smartest city in the world” looks forward to using such vehicles. “The skies over Dubai could become uncomfortably crowded very quickly. The ground level of the city could become a dark place of intrigue and mystery like *Blade Runner*,” said Noel Sharkey, computer scientist and robotics expert at Sheffield University. Jane Wakefield, *Dubai Tests Drone Taxi Service*, BBC NEWS (Sept. 26, 2017), <https://www.bbc.com/news/technology-41399406>.

given permission to fly through most U.S. airspace.”⁴ Clearly in agreement with that sentiment, William H. Merideth was arrested after shooting at a drone, flown by his neighbor John David Boggs, that was hovering over his backyard and spying on his 16-year-old daughter while she was sunbathing by the pool.⁵ Merideth has adopted the moniker the “Drone Slayer” and asserted that Boggs invaded his and his family’s privacy when the drone took a video of his daughter.⁶ Boggs admitted that he was recording video but released the flight data recorder, which shows the drone’s path at 193 feet above the ground.⁷ He asserted that “for sure [it] didn’t descend down to no 10 feet, or look under someone’s canopy, or at somebody’s daughter.”⁸ Ironically, the incident occurred in Bullitt County, Kentucky, where Merideth was cleared of first-degree endangerment and criminal mischief charges, with the judge opining that Merideth “had the right to shoot this drone.”⁹

Merideth and other landowners want to know how to keep drones away from their property or what civil redress is available to them for unwelcome drones. Do existing property laws addressing trespass and nuisance sufficiently protect landowners from unwanted drones?¹⁰ What rights and remedies are available to landowners to curtail intrusive drone use? How can business owners prevent physical injury to their property¹¹

4. AARON SMITH, PEW RES. CTR., U.S. VIEWS OF TECHNOLOGY AND THE FUTURE 3 (2014), <http://www.pewresearch.org/wp-content/uploads/sites/9/2014/04/US-Views-of-Technology-and-the-Future.pdf>.

5. WAVE, an NBC affiliate, reported that Bullitt County Judge Rebecca Ward asserted that the drone invaded the Merideths’ privacy and that “they had the right to shoot this drone.” Elisha Fieldstadt, *Case Dismissed Against William H. Merideth, Kentucky Man Arrested for Shooting Down Drone*, NBC NEWS (Oct. 27, 2015, 1:28 PM), <https://www.nbcnews.com/news/us-news/case-dismissed-against-william-h-merideth-kentucky-man-arrested-shooting-n452281> (“Merideth was cleared of first-degree endangerment and criminal mischief charges . . .”).

6. Miriam McNabb, *The Kentucky “Drone Slayer” Case Dismissed*, DRONELIFE (Mar. 22, 2017), <https://dronelife.com/2017/03/22/kentucky-drone-slayer-case-dismissed/>.

7. Gil Corsey, *Update: Drone Owner Disputes Shooter’s Story; Produces Video He Claims Shows Flight Path*, WDRB (July 30, 2015, 11:57 AM), <http://www.wdrb.com/story/29670583/update-drone-owner-disputes-shooters-story-produces-video-he-claims-shows-flight-path>.

8. *Id.*

9. McNabb, *supra* note 6.

10. The creators of the trespass tort could not possibly have conceived of the invention of drones because “[t]respass is one of the oldest torts known to Anglo-American jurisprudence, dating as far back as twelfth-century England.” Int’l Union of Painters & Allied Trades Dist. Council 15 Local 159 v. Great Wash Park, LLC, No. 67453, 2016 WL 4499940, at *6 (Nev. Ct. App. Aug. 18, 2016) (Tao, J., concurring).

11. See, e.g., Leslie Kaufman & Ravi Somaiya, *Drones Offer Journalists a Wider View*, N.Y. TIMES, Nov. 25, 2013, at B1 (describing drones crashing into Manhattan skyscrapers and falling to the sidewalk).

and secure their property to block drones from potentially obtaining confidential information from a drone flyover? And how do state and federal regulators manage the challenges of navigation, hardware reliability, and airspace management?¹²

These examples demonstrate that while the legal implications of the increasing prevalence of drones overhead embrace a broad array of torts and crimes ranging from invasion of privacy to industrial espionage, the focus here will be limited primarily to the tort of trespass to land. Part I of this Article will discuss what drones are and how they are used. Part II will provide the history of airspace rights, current regulation, and the challenges of integrating drones into the airspace. Parts III, IV, and V, will explore the state and local regulation of drones, including the viability of trespass and other state law torts that arise from the use of drones. Finally, Part VI will examine the future of drone use, including a possible implication of cryptocurrency tokens.

I. WHAT ARE DRONES AND HOW ARE THEY USED?

A. *What Are Drones?*

A drone is an unpiloted aircraft also known as an “unmanned aerial vehicle” (UAV).¹³ When expanded to include its remote controls, the ensemble is an “unmanned aircraft system” (UAS).¹⁴ There are two main classifications when it comes to drones in the United States: recreational drones, also known as “small hobbyist” drones, and commercial drones.¹⁵

UAVs can use engines powered by either a gasoline and oil mixture similar to those in lawn mowers, or gas engines like those used in cars. However, electric motors, which use energy from batteries, solar cells, or

12. The FAA found that drone sightings by United States air traffic facilities increased to 1,274 between February and September 2016 compared to 874 drone sightings for the same period in 2015. In addition to the incident between an Army UHB-60 Black Hawk helicopter carrying security officials to the United Nations and a Phantom 4 drone in New York City, there was a near-miss incident between a Lufthansa passenger jet at LAX and a drone flying in the approach corridor. Trevor Mogg, *A Phantom 4 Drone Hit a Helicopter over New York and the Drone Came Out Worse*, DIGITAL TRENDS (Oct. 5, 2017, 11:55 PM), <https://www.digitaltrends.com/cool-tech/drone-helicopter-new-york-collision/>.

13. Elizabeth Howell, *What Is a Drone?*, SPACE (Oct. 3, 2018, 2:32 PM), <https://www.space.com/29544-what-is-a-drone.html> (“Drones have been around for almost as long as airplanes have been used in warfare (1911), and that’s not even including bomb-filled balloons that were first used by Austria in the mid-1800s.”).

14. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331(8) 126 Stat. 11, 72 (2012); 14 C.F.R. § 107.3.

15. Andrew Meola, *The FAA Rules and Regulations You Need to Know to Keep Your Drone Use Legal*, BUS. INSIDER (July 25, 2017, 1:12 PM), <http://www.businessinsider.com/drones-law-faa-regulations-2017-7>.

fuel cells, are increasingly popular.¹⁶ Hobbyists may pay up to \$500 for a UAS that includes the UAV, batteries, chargers, and the remote control.¹⁷ Sometimes, the control is by a smartphone app rather than a separate device.¹⁸ Generally, the basic drones can fly for “up to 10 minutes on a battery charge at up to 22 mph, with a range of about 150–200 feet.”¹⁹ As the hobby interest increases, prices could move toward \$2,000 for more elaborate drones, which may include a camera.²⁰ These better UAVs may be able to remain airborne for twenty-five minutes with a range of half a mile.²¹ “Commercial users may pay \$10,000 or more” for UAVs that will stay airborne longer with an extended range and payload-carrying capability.²² They also are often quieter than the low-end UAVs.²³

B. *How Are Drones Used?*

Drones can change the way businesses operate and the way hobbyists enjoy technology, enabling them to see the world from a bird’s-eye view. Hobbyists and commercial operators often use drones for aerial photography purposes.²⁴ Photography can range from families taking overhead pictures of a backyard barbeque, to real estate agents taking pictures for a home listing, to professional videographers filming a documentary, and to anything in between. Skyris Imaging, an aerial photography, video, and GIS company, does not take residential real estate companies as clients to avoid flying drones over private property.²⁵ According to its owner, Joe Vaughn, his company’s focus is on commercial clients, which reduces the potential privacy issues.²⁶

It will not be long until businesses are using drones in the shipment

16. BILL CANIS, CONG. RES. SERV., UNMANNED AIRCRAFT SYSTEMS (UAS): COMMERCIAL OUTLOOK FOR A NEW INDUSTRY 4 (2015), <https://fas.org/sgp/crs/misc/R44192.pdf>.

17. *Id.* at 5.

18. *Id.* at 4.

19. *Id.*

20. *Id.*

21. *Id.*

22. *Id.*

23. *Id.* at 7 (“The drone, weighing less than an ounce, can hover silently for more than eight minutes . . .”).

24. See David Schloss, *Drones for Photography*, OUTDOOR PHOTOGRAPHER (Aug. 8, 2017), <https://www.outdoorphotographer.com/photography-gear/cameras/drones-for-photography/#>.

25. See Christina Sterbenz, *Should We Freak Out About Drones Looking in Our Windows?*, BUS. INSIDER (Sept. 24, 2014, 2:22 PM), <http://www.businessinsider.com/privacy-issues-with-commercial-drones-2014-9>.

26. *Id.* (“If I were to point [a drone] at somebody’s window, I’d have to be within feet to see anything . . .”).

and delivery of their products.²⁷ Companies like Amazon have bold plans to send drones from distribution centers directly to customer's homes to deliver products, which would require flight patterns through residential areas.²⁸ In fact, on December 7, 2016, Amazon made its first commercial drone delivery.²⁹ Google, UPS, FedEx, and various startups are also considering the possibilities of drone usage.³⁰ Of course, that could raise some problems with the neighbors. While the recipient may agree to a drone delivery, just like implied consent for a ground delivery from FedEx or UPS, the neighbors may not want to have the delivery drone flying over their backyard to reach the recipient's property.

Meteorologists have been using drones to help predict severe weather because drones equipped with special meteorological sensing equipment expedite the forecasting process.³¹ The ability of drones to monitor areas that are out of reach for ground-based instruments and altitudes below where satellites are effective make them extremely attractive in the weather industry as well as in weather-related rescue efforts. Additionally, drones are increasingly being used by organizations to assist disaster management operations. The American Red Cross has begun using drones to assist relief efforts after hurricanes, tornadoes, and other natural disasters.³² Drones can help locate missing individuals and assess which areas need the most aid. Drones also help evaluate monetary

27. See Jack Nicas, *Corporate News: Amazon Asks FAA for Permission to Test Drones*, WALL ST. J. (July 11, 2014, 7:28 PM), <https://www.wsj.com/articles/amazon-asks-faa-for-permission-to-fly-drones-1405088198>; see also Lois Weiss, *Amazon Eyes Midtown Lair on Avenue of the Americas*, N.Y. POST (July 16, 2014, 6:42 AM), <https://nypost.com/2014/07/16/amazon-eyes-midtown-lair-on-avenue-of-the-americas/>. (suggesting that the 285,000 square foot facility Amazon was purportedly targeting would allow Bezos to test out drone deliveries).

28. *Amazon Prime Air*, AMAZON, <https://www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011> (last visited Oct. 24, 2018).

29. Jamie Condliffe, *An Amazon Drone Has Delivered Its First Products to a Paying Customer*, MIT TECH. REV. (Dec. 14, 2016), <https://www.technologyreview.com/s/603141/an-amazon-drone-has-delivered-its-first-products-to-a-paying-customer/> (reporting that Amazon delivered an Amazon Fire TV stick and a bag of popcorn—a lightweight payload—and that the test was conducted in Cambridge, U.K. because of challenges presented by FAA regulations requiring that drones fly within the line of sight).

30. Will Knight, *Sorry, Shoppers: Delivery Drones Might Not Fly for a While*, MIT TECH. REV. (Mar. 30, 2016), <https://www.technologyreview.com/s/601117/sorry-shoppers-delivery-drones-might-not-fly-for-a-while/> (noting that since the FAA still prohibits commercial drone flights, these companies must all seek exemptions to proceed with their testing).

31. Jamie Leventhal, *Storm Drones Could Revolutionize Weather Forecasting*, QUARTZ (July 6, 2017), <https://qz.com/1022076/storm-drones-could-revolutionize-weather-forecasting/>.

32. Chris Morris, *Here's How the Red Cross Is Using Drones for Disaster Relief*, FORTUNE (Sept. 8, 2017), <http://fortune.com/2017/09/08/red-cross-drones-houston-harvey/>.

damages for insurance purposes, which is a key component of a city's aid package.³³

The private sector is using drones for such rescue efforts as well. Zipline, a company formed by Silicon Valley entrepreneurs, operates the "world's only drone delivery system at national scale to send urgent medicines, such as blood and animal vaccines, to those in need—no matter where they live."³⁴ Zipline currently operates within the African nation of Rwanda, making fifty to 150 deliveries per day using fifteen UAVs.³⁵ According to Margaret Chan, director general of the World Health Organization, "[t]his visionary project in Rwanda has the potential to revolutionize public health, and its life-saving potential is vast."³⁶ Interestingly, one of the poorest countries in the world³⁷ gets to take advantage of burgeoning technology because it is not burdened by the strict regulations and safety concerns that often delay progress in more well-developed countries.³⁸ The United States worries about reliability, safety, and air traffic control issues, among other concerns. Nicholas Roy, an MIT professor, notes that "[y]ou have to assume [drones will] fall out of the sky. So how do you make sure these vehicles are reliable enough—both the hardware and the software?"³⁹

Rescue efforts with drones are also made by journalists. "What drones give you is anywhere, anytime access to the sky. . . . That perspective is something a journalist just wouldn't have unless he waited for officials, or hired a plane," according to Chris Anderson, who now runs a drone

33. See *id.*; see also Alexandria Tomanelli, *A Drone's Eye View: Why and How the Federal Aviation Administration Should Regulate Hobbyist Drone Use*, 34 *TOURO L. REV.* 867, 875–76 (2018) (discussing the FAA's use of drones to conduct damage assessments of infrastructure, homes, and rail lines in Texas after Hurricane Harvey passed through).

34. Zipline, *Lifesaving Deliveries by Zipline Drone in Rwanda*, *MIAMI HERALD* (Feb. 8, 2018, 6:49 PM), <https://www.miamiherald.com/news/business/article198436619.html>.

35. Will Knight, *Why Rwanda Is Going to Get the World's First Network of Delivery Drones*, *MIT TECH. REV.* (Apr. 4, 2016), <https://www.technologyreview.com/s/601190/why-rwanda-is-going-to-get-the-worlds-first-network-of-delivery-drones/>.

36. *Id.*

37. John Markoff, *Drones Marshaled To Drop Lifesaving Supplies over Rwandan Terrain*, *N.Y. TIMES* (Apr. 4, 2016), <https://www.nytimes.com/2016/04/05/technology/drones-marshaled-to-drop-lifesaving-supplies-over-rwandan-terrain.html> (noting that in 2014, the International Monetary Fund ranked Rwanda 170th for gross domestic product).

38. *Id.* (reporting that Michael Fairbanks, a member of the Rwandan president Paul Kagame's presidential advisory council, applauded the ability of Rwanda to make a quick decision); see also Linda Chiem, *Drone Test Sites Give States Expanded Regulatory Role*, *LAW360* (May 23, 2018, 7:29 PM), <https://www.law360.com/articles/1046392/drone-test-sites-give-states-expanded-regulatory-role> ("Put bluntly, federal regulators are not operating with the urgency necessary to keep abreast of industry development . . .").

39. Knight, *supra* note 30.

company after being an editor of *Wired* magazine.⁴⁰ But it is not just about getting the story. For example, British photographer Lewis Whyld launched a drone to film the destruction following Typhoon Haiyan in the Philippines, and in the process, discovered two bodies that were later recovered.⁴¹ Whyld's footage was broadcast on CNN, but the Associated Press, News Corporation, and the BBC have used drones to show the scale of large disasters as well.⁴²

After all, UAVs can fly in tighter spaces than helicopters, are far less expensive, and can hover closer to the targeted area—making them incredibly useful in search and rescue operations.⁴³ One example occurred in January 2018 when two young men were caught in turbulent waves outside Sydney, Australia. Australian lifeguards noticed the men during a practice session with the drone and dropped an inflatable “rescue pod” that helped save the young men.⁴⁴ The use of drones for similar operations will likely explode in the future.

Drones also give paparazzi a new way to follow and photograph celebrities.⁴⁵ There are so many opportunities for drones in journalism that universities have started drone journalism courses.⁴⁶

Geographic Information Systems have utilized drones to deliver “high-resolution images in near real time.”⁴⁷ The ability of drones to fly at altitudes much lower than manned aircraft enable researchers to survey

40. Kaufman & Somaiya, *supra* note 11.

41. *Id.*

42. *Id.*

43. Carl Franzen, *Canadian Mounties Claim First Person's Life Saved by a Police Drone*, VERGE (May 10, 2013, 12:23 PM), <https://www.theverge.com/2013/5/10/4318770/canada-dragonflyer-drone-claims-first-life-saved-search-rescue> (reporting that in 2013, an injured driver stranded in a snowy area of Saskatchewan, Canada, was located by Canadian police using a Dragonflyer X4-ES drone with an infrared camera after a helicopter search failed); Keith Nelson Jr., *Drones Can Help When Disaster Strikes, but Only When They're Allowed to*, DIGITAL TRENDS (Sept. 28, 2017, 3:00 AM), <https://www.digitaltrends.com/cool-tech/rescue-drones-hurricane-flood-disaster-relief/> (reporting that a recent study concluded drones helped save one life per week and noting that in 2015, the Auburn, Maine Fire Department used a DJI Phantom 3 to drop down life vests to an 18-year-old man stranded in the middle of the river).

44. Isabella Kwai, *A Drone Saves Two Swimmers in Australia*, N.Y. TIMES (Jan. 18, 2018), <https://www.nytimes.com/2018/01/18/world/australia/drone-rescue-swimmers.html>.

45. Kaufman & Somaiya, *supra* note 11 (reporting that a drone flew over singer Tina Turner's private wedding in Switzerland in August 2013 and that on another occasion, a picture of singer Beyoncé was captured by a drone on a roller coaster at Coney Island).

46. *Id.* (listing the University of Missouri, University of Nebraska, and the Tow Center for Digital Journalism at Columbia University as institutions with such programs but noting that such programs must seek permission from the FAA for their educational flights); *see also infra* note 226.

47. *How Are Surveying Drones Taking GIS Mapping to The Next Level?*, IDENTIFIED TECHS. (Oct. 21, 2017, 2:46 PM), <https://www.identifiedtech.com/blog/construction-uav/how-are-surveying-drones-taking-gis-mapping-to-the-next-level/>.

land with much greater accuracy than ever before.⁴⁸ Further, drones provide cheaper production costs in addition to superior survey photography capabilities.⁴⁹ Drones also have significantly reduced the time and cost of performing building inspections because they can perform facade inspections, roof inspections, and moisture inspections by attaching thermal imaging cameras.⁵⁰

The benefit of drones has become apparent in recent years within the farming industry. Farmers have used drones in several ways, from ranging and surveying property to crop dusting and spraying crops.⁵¹ Forecasters predict drones sold for agricultural use will dramatically increase in the future. The American Farm Bureau estimated that farmers using drone services to monitor their crops could see a return on their investment of \$12 per acre for corn, \$2.60 per acre for soybeans, and \$2.30 per acre for wheat.⁵² Eventually, farmers might use UAVs for targeted application of herbicides and pesticides.⁵³

The Teal Group, a United States aerospace consulting firm, sees a strong potential for growth.⁵⁴ It believes UAVs are “the most dynamic growth sector of the world aerospace industry,” and “[n]ew unmanned combat aerial vehicle programs, commercial, and consumer spending all promise to drive more than a tripling of the market over the next decade.”⁵⁵ For example, Boeing has unveiled a cargo delivery drone prototype that could transform the logistics industry.⁵⁶ Boeing’s new drone weighs nearly 750 pounds and could transport a load around 500 pounds.⁵⁷ Cargo transport drones could help deliver time-sensitive and high-value goods for individuals or organizations.

48. *Id.*

49. *Id.*

50. Adam Frumkin, *Drones: The Future of Building Inspections*, KIPCON (Feb. 26, 2017), <http://kipconengineering.com/drone-building-inspections/>.

51. Andrew Meola, *Exploring Agricultural Drones: The Future of Farming Is Precision Agriculture, Mapping, and Spraying*, BUS. INSIDER (Aug. 1, 2017, 2:33 PM), <http://www.businessinsider.com/farming-drones-precision-agriculture-mapping-spraying-2017-8>.

52. Matt Hopkins, *American Farm Bureau Federation, Measure Launch Drone ROI Calculator*, PRECISIONAG (July 21, 2015), <https://www.precisionag.com/systems-management/data/american-farm-bureau-federation-launches-drone-roi-calculator/>.

53. Marco Margaritoff, *North Dakota State University's Herbicide-Spraying Drone Covers 33 Acres in an Hour*, DRIVE (July 23, 2018), <https://www.thedrive.com/tech/22348/north-dakota-state-universitys-herbicide-spraying-drone-covers-33-acres-in-an-hour>.

54. *UAV Production Will Total \$93 Billion*, TEAL GROUP CORP. (Aug. 17, 2015), <http://www.tealgroup.com/index.php/pages/press-releases/34-uav-production-will-total-93-billion>.

55. *Id.*

56. Lewis King, *Boeing's Cargo UAV a Shot in the Arm for Drone Delivery Market*, AIR CARGO WORLD (Jan. 11, 2018), <https://aircargoworld.com/allposts/boeings-cargo-uav-a-shot-in-the-arm-for-drone-delivery-market-video/>.

57. *Id.*

II. AIRSPACE RIGHTS

A. *Trespass*

So, what's the problem? Landowners may not want drone traffic over their private property and may seek remedies, civil and criminal, to keep drones away from their property. The question then is whether a drone flying over a landowner's property constitutes a trespass. Courts have long held that a trespass occurs when a person or object interferes with the owner's exclusive possession and control of the land.⁵⁸ But in the case of drones, we are not talking about trespass of the physical land, but rather trespass of the airspace above the land. This requires the trespasser to enter into the immediate reaches of the airspace and interfere substantially with the landowner's use and enjoyment of the land.⁵⁹

B. *History of Airspace Rights*

While one generally thinks of trees, water, and animals as the planet's natural resources, airspace is one of the most abundant natural resources. Just as location is important in evaluating the value of land, whether that airspace is a beach view or is navigable airspace used by commercial jets, the location of that airspace is a large determinant of its value. And while it is abundant, it is finite and must be respected and shared.

The property rights of landowners in the airspace above their real property largely began to be addressed in the fourteenth century with the doctrine of "cujus est solum, ejus usque ad coelum."⁶⁰ The doctrine translates to "whoever owns the ground, owns it all the way from heaven to hell."⁶¹ This belief was fused into English and American common law

58. See RESTATEMENT (SECOND) OF TORTS § 158 (AM. LAW. INST. 1965) ("One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally (a) enters land in the possession of the other, or causes a thing or a third person to do so, or (b) remains on the land, or (c) fails to remove from the land a thing which he is under a duty to remove."); see also CAL. CIV. CODE § 1708.8(a) (West 2016) ("A person is liable for physical invasion of privacy when the person knowingly enters onto the land or into the airspace above the land of another person without permission or otherwise commits a trespass in order to capture any type of visual image, sound recording, or other physical impression of the plaintiff engaging in private, personal, or familial activity and the invasion occurs in a manner that is offensive to a reasonable person.").

59. See RESTATEMENT (SECOND) OF TORTS § 159(2) (AM. LAW. INST. 1965) ("Flight by 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.").

60. See generally Yehuda Abramovitch, *The Maxim "Cujus Est Solum Ejus Usque Ad Coelum" as Applied in Aviation*, 8 MCGILL L.J. 247, 247–65 (1962).

61. Luna Vanderispaillie, *Does Your Property Reach Heaven's Gates? An International Legal Perspective*, UNIFLY (Aug. 7, 2017), <https://www.unifly.aero/news/does-your-property-reach-heavens-gates>.

in the seventeenth and eighteenth centuries due in large part to Edward Coke and William Blackstone's instrumental commentaries.⁶²

Airspace rights needed legal clarification once airplanes and air travel became common in everyday life. Can you imagine if every airline had to request permission⁶³ from every property owner along a route in order to fly through their airspace? The Air Commerce Act of 1926,⁶⁴ as amended in the Civil Aeronautics Act of 1938,⁶⁵ established the federal air highway. Currently, although 49 U.S.C. § 40103(a)(1) states that “[t]he United States Government has exclusive sovereignty of airspace of the United States,” subsection 2 recognizes public use of airspace only above “navigable airspace,” thereby retaining private ownership below “navigable airspace.”⁶⁶ The ownership and use of airspace rights is significant in today's society in the context of view easements, solar access easements, flight path easements, and development rights in the non-navigable airspace above an owner's land. Property rights and their associated air rights have evolved at a blistering pace in modern times due to many technological innovations. With the birth of high-rise buildings and other architectural advancements, airspace has become increasingly valuable.⁶⁷ Airspace over land in the middle of wide open spaces in Alaska may be of little value, but a small amount of airspace in the heart of Manhattan is likely worth a fortune.⁶⁸ In recent years, the innovation and popularity of drones has blurred the lines of navigable airspace and property rights to an even greater degree.⁶⁹

62. Troy A. Rule, *Airspace in a Green Economy*, 59 UCLA L. REV. 270, 278–79 (2011).

63. Such a permission would be an aviation easement, which would “allow aircraft to fly through a given airspace.” *City of Westchester v. Town of Greenwich*, 793 F. Supp. 1195, 1204 (S.D.N.Y. 1992), *rev'd sub nom.* *City of Westchester v. Comm'r of Transp.*, 9 F.3d 242 (2d Cir. 1993).

64. Air Commerce Act of 1926, Pub. L. No. 69-254, 44 Stat. 568.

65. Civil Aeronautics Act of 1938, Pub. L. No. 75-706, 52 Stat. 973.

66. 49 U.S.C. § 40103(a)(1)–(2) (2018).

67. Martin A. Schwartz, *It's Up in the Air: Air Rights in Modern Development*, FLA. B.J., Apr. 2015, at 42, <https://www.floridabar.org/the-florida-bar-journal/its-up-in-the-air-air-rights-in-modern-development/>.

68. Twenty years ago, \$45 a square foot was considered a reasonable fee for air rights in New York, but in recent years, that figure has risen to \$450 per square foot in prime neighborhoods. Robin Finn, *The Great Air Race*, N.Y. TIMES (Feb. 22, 2013), <https://www.nytimes.com/2013/02/24/realestate/the-great-race-for-manhattan-air-rights.html>. The value of sunlight for solar panels is an increasing concern, New Mexico and Wyoming even prohibit interference with solar panels. *See* N.M. STAT. ANN. § 47-3-4(B)(1) (2019); WYO. STAT. ANN. § 34-22-103(b)(i) (2019).

69. Andrea Peterson & Matt McFarland, *You May Be Powerless to Stop a Drone from Hovering over Your Own Yard*, WASH. POST (Jan. 13, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/01/13/you-may-be-powerless-to-stop-a-drone-from-hovering-over-your-own-yard/?utm_term=.cc6909ac86e8.

In 1946, the Supreme Court of the United States provided guidance on where navigable airspace begins and private property ends in the landmark case *United States v. Causby*.⁷⁰ The Causbys were farmers living adjacent to a military airport that had aircraft flying as low as eighty-three feet above their land.⁷¹ The deafening noise of aircraft caused their chickens great harm and resulted in them killing themselves by flying into the walls.⁷² The Supreme Court's decision brought forth two key principles regarding airspace while maintaining the public air highway in its holding.⁷³ First, landowners have "exclusive control of the immediate reaches of the enveloping atmosphere."⁷⁴ Second, "the landowner owns at least as much of the space above the ground as he can occupy or use."⁷⁵

C. FAA Regulation of Airspace

Pursuant to the Federal Aviation Act of 1958, the FAA has the right to regulate airspace.⁷⁶ The FAA has clearly defined six major classifications of regulated airspace, including both controlled airspace (Class A through Class E) and uncontrolled airspace (Class G).⁷⁷

Regulated, controlled airspace includes the following classes:

70. *United States v. Causby*, 328 U.S. 256, 258 (1946).

71. *Id.*

72. *Id.* at 259.

73. *Id.* at 260–61 ("It is ancient doctrine that at common law ownership of the land extended to the periphery of the universe But that doctrine has no place in the modern world. The air is a public highway Were that not true, every transcontinental flight would subject the operator to countless trespass suits.").

74. *Id.* at 264.

75. *Id.* In addition, the Federal Aviation Act of 1958 expanded the statutory definition of "navigable airspace" from 500 feet above ground level to include all "airspace needed to insure safety in take-off and landing of aircraft." Federal Aviation Act of 1958, Pub. L. No. 85-726, § 101(24), 72 Stat. 731, 739; *see also* 14 C.F.R. § 77.23 (2019). "Navigable airspace" is defined as "airspace above the minimum altitudes of flight prescribed by regulations [but also] including airspace needed to ensure safety in the takeoff and landing of aircraft." 49 U.S.C. § 40102(a)(32) (2019). In other words, "The FAA is responsible for the safety of U.S. airspace from the ground up." *Busting Myths About the FAA and Unmanned Aircraft*, FED. AVIATION ADMIN., <https://www.faa.gov/news/updates/?newsId=76240> (last updated Mar. 7, 2014).

76. Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 731.

77. FED. AVIATION ADMIN., PILOT'S HANDBOOK OF AERONAUTICAL KNOWLEDGE 15-2–3 (2016), https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/phak/media/pilot_handbook.pdf.

Class A airspace is classified as any airspace over 18,000 feet above mean sea level (“MSL”), and aircraft operating in this airspace need to operate via instrumental flight rules.⁷⁸

Class B airspace is classified as airspace from surface level up to 10,000 feet above MSL. This airspace surrounds the nation’s busiest airports and requires air traffic control (“ATC”) clearance to enter.⁷⁹

Class C airspace is similar to Class B airspace and includes airspace from surface level up to 4,000 feet above the airport elevation charted in MSL. Aircraft operators must maintain two-way ATC communication before entering.⁸⁰ Class C airspace does not surround the nation’s busiest airports, but it surrounds those airports that operate with control towers, radar approach control, and instrumental flight rules.

Class D airspace covers the airspace around the smallest airports from surface level up to 2,500 feet above the airport elevation charted in MSL. Like Class C airspace, Class D airspace requires any aircraft operator to establish two-way ATC communication before entering.⁸¹

Class E airspace is all controlled airspace not included in Class A through Class D airspaces. Most areas of Class E airspace begin at 1,200 feet above ground level up to the beginning of Class A airspace at 18,000 feet above MSL.⁸² Many other locations of Class E airspace begin at 700 feet above ground level.

Regulated, but uncontrolled airspace:

Class G uncontrolled airspace extends from the surface up to the beginning of the overlying Class E airspace, which many times is either 1,200 feet or 700 feet above MSL. Pursuant to the FAA Modernization and Reform Act of 2012, UAV operators are required to fly their aircraft in Class G airspace.⁸³

UAV operators must be conscious of approaching Class B airspace near airports, even at heights of only a few hundred feet above MSL. Much of New York City has Class B controlled airspace since there are

78. *Id.* at 15-2.

79. *Id.*

80. *Id.*

81. *Id.*

82. *Id.* at 15-2-3.

83. *Id.* at 15-3.

three nearby airports (LaGuardia, JFK, and Newark).⁸⁴ In addition, there are Special Flight Rules, which most drones cannot comply with, limiting flights above the Hudson and East Rivers, and there is a temporary flight restriction over President Trump's family residence.⁸⁵ This makes flight by UAVs in Manhattan very difficult.

While Los Angeles has a major international airport, there are also many smaller airports surrounded by controlled airspace, much of which is Class D—the airspace with the most waivers.⁸⁶ This is helpful for the dozens of film, television, and news companies that want to use that airspace. Many open areas in the broad Los Angeles area are available to drone flights, including downtown Los Angeles.⁸⁷ Drones are an efficient means to obtain aerial shots, whether for news or entertainment, and Hollywood producers are eager to explore uses for the new technology. Unlike news agencies trying to capture an unfolding event, film and television productions work on a schedule and can apply for authorizations and waivers as needed.

D. *Integration of UAVs into the United States Airspace*

The FAA Modernization and Reform Act of 2012 required that the FAA safely integrate UAVs into the United States airspace by September 30, 2015.⁸⁸ Recognizing that recreational drones are by far the most common and numerous, the FAA decided that each recreational drone over 0.55 pounds must be registered with the FAA.⁸⁹ The FAA estimates that there were around 1.1 million recreational drones in 2016, with estimates for that amount to increase to as high as 2.94 million by 2021.⁹⁰ However, since many recreational drones are less than 0.55 pounds and thus do not meet the registration requirement,⁹¹ the FAA's estimate is very limited. The Consumer Technology Association (CTA) reported that there were 2.4 million recreational drones sold in 2016, more than double

84. Eric Ringer, *Drone Airspace in America's Largest Media Markets*, SKYWARD (Aug. 16, 2017), <https://skyward.io/drone-airspace-in-americas-largest-media-markets/>.

85. *Id.*

86. *Id.*; see also Tariq Rashid, *How to Apply for a Part 107 Waiver*, SKYWARD (Mar. 1, 2017), <https://skyward.io/how-to-apply-for-a-part-107-waiver-from-the-faa-the-right-way/> (noting types and procedure for waivers).

87. Ringer, *supra* note 84.

88. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(a)(3) 126 Stat. 11, 73 (2012).

89. See *FAADroneZone*, FED. AVIATION ADMIN., <https://faadronezone.faa.gov/#/> (last visited Sept. 3, 2019).

90. FED. AVIATION ADMIN., *supra* note 1, at 40–41.

91. See Andrew Meola, *Drone Market Shows Positive Outlook with Strong Industry Growth and Trends*, BUS. INSIDER (July 13, 2017, 10:42 AM), <http://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts-2017-7>.

the FAA's estimate.⁹² This figure takes into account all recreational drones, no matter the size. The CTA also estimates that recreational drone sales could increase to 29 million by 2021.⁹³

To use a small UAS, one must register it with the FAA, pay a \$5 fee, and have a remote pilot certification with a small UAS rating.⁹⁴ However, obtaining the certification is not enough to understand the law related to operating a UAS; it is incumbent upon the pilot to take extra care to understand this law. In fact, "the FAA strongly encourages all UAS pilots to check local and state laws before gathering information through remote sensing technology or photography" because privacy issues are beyond the FAA's scope.⁹⁵ However, the FAA does "provide all drone users with recommended privacy guidelines as part of the UAS registration process and through the FAA's B4UFly mobile app."⁹⁶

In June 2016, the FAA issued the final rule for drone operation, known as Part 107, which set the parameters for commercial use of drones weighing up to 55 pounds.⁹⁷ The regulations state that commercial drones:

- Can only be operated during daytime or civil twilight while with appropriate anti-collision lighting;
- Can only be operated up to a maximum of 400 feet above the ground level. If operated from a structure, it must be within 400 feet of the structure;
- Cannot be operated from a moving aircraft;
- Cannot be operated from a moving vehicle unless it's being operated over sparsely populated areas;
- Can only be operated when weather visibility is at least three miles from the control station;
- With an ATC permission, can be operated in Class B, C, D, and E airspaces;

92. *Id.*

93. *Id.*

94. See 14 C.F.R. § 107.12–13 (2017); *Register Your Drone*, FED. AVIATION ADMIN., https://www.faa.gov/uas/getting_started/register_drone/ (last updated July 11, 2019, 8:56 AM); see also Juan Plaza, *FAA Remote Pilot Certification Reaches an Important Milestone*, COMM. UAV NEWS (Aug. 7, 2018), <https://www.expouav.com/news/latest/faa-remote-pilot-certificates-milestone/> ("On July 26th the Federal Aviation Administration (FAA) announced that more than 100,000 people have obtained a Remote Pilot Certificate to fly a drone for commercial and recreational uses (not qualifying as 'model aircraft').").

95. *Fact Sheet—Small Unmanned Aircraft Regulations (Part 107)*, FED. AVIATION ADMIN. (June 21, 2016), https://www.faa.gov/news/fact_sheets/news_story.cfm?newsID=20516.

96. *Id.*

97. 14 C.F.R. § 107.3 (2019).

- Can be operated in a Class G airspace even without ATC permission;
- While in operation, must remain in the Visual-Line-Of-Sight.⁹⁸

Commercial drone operators can request a waiver from these restrictions.⁹⁹ However, that can be time-consuming, often taking months, since the FAA receives more than 3,000 waiver requests per week “with a backlog in the tens of thousands.”¹⁰⁰

Commercial drones operate to satisfy a wide variety of business activities. Pilots for commercial drones must satisfy each of the following requirements: have a Remote Pilot Airman Certification, be at least sixteen years old, and pass vetting by the Transportation Security Administration.¹⁰¹ Like recreational drones over 0.55 pounds, every commercial drone must be registered with the FAA and have a unique registration number for each aircraft.¹⁰² The FAA estimated that roughly 42,000 commercial drones were in use in 2016 and that by 2021, 442,000 to 1.6 million commercial drones would be operating.¹⁰³ The FAA also estimated that there were 73,000 commercial drone pilots by the end of 2017 and that the number of pilots would increase to almost 400,000 pilots by 2022.¹⁰⁴ For comparison, BI Intelligence estimated commercial drone shipments in 2016 at 102,600, nearly double the FAA’s estimate.¹⁰⁵ BI Intelligence also estimates that by 2021, the number of commercial drone shipments will increase by 51% to 805,000.¹⁰⁶ The challenge then

98. 14 C.F.R. §§ 107.11, .25, .29, .31, .41, .51 (2019).

99. Waiver requests cover several scenarios. *Part 107 Waivers*, FED. AVIATION ADMIN., https://www.faa.gov/uas/commercial_operators/part_107_waivers/ (last updated Aug. 1, 2019); Rashid, *supra* note 86.

100. Rebecca Wilson, *Q&A: How Skyward Is Working with the FAA on LAANC*, SKYWARD (Aug. 7, 2017), <https://skyward.io/qa-how-skyward-is-working-with-the-faa-on-laanc/>.

101. *Summary of Small Unmanned Aircraft Rule (Part 107)*, FED. AVIATION ADMIN. (June 21, 2016), https://www.faa.gov/uas/media/Part_107_Summary.pdf; *Drone Certification: A Step-by-Step Guide to FAA Part 107 for U.S. Commercial Drone Pilots*, UAV COACH, <https://uavcoach.com/drone-certification/#1> (last visited Apr. 4, 2019).

102. *Register Your Drone*, FED. AVIATION ADMIN., https://www.faa.gov/uas/getting-started/register_drone/ (last updated July 11, 2019, 8:56 AM).

103. David Shepardson, *U.S. Commercial Drone Use to Expand Tenfold by 2021: Government Agency*, REUTERS (Mar. 21, 2017, 4:22 PM), <https://www.reuters.com/article/us-usa-drones/u-s-commercial-drone-use-to-expand-tenfold-by-2021-government-agency-idUSKBN16S2NM> (reporting statements by the FAA regarding the growing use of commercial drones as the regulatory framework surrounding them evolves).

104. FED. AVIATION ADMIN., *supra* note 1, at 44–45.

105. Meola, *supra* note 91.

106. *Id.*

is regulating airspace in a manner that will permit the use of drones without interfering with landowners' property rights.¹⁰⁷

E. Penalties for Unregistered Drones

According to Michael Braasch, an electrical engineering professor and drone expert at Ohio University, one challenge with novice drone operators is that they are often “blissfully unaware” of aviation safety practices.¹⁰⁸ The FAA has partnered with the drone industry on a public awareness campaign, *Know Before You Fly*, which disseminates safety rules to hobbyist flyers. In addition, the B4UFly application serves the same purpose.¹⁰⁹ The industry is also encouraging manufacturers to put warning labels on the UAS itself, reminding operators to research and follow safety regulations.¹¹⁰

Drone owners need only spend \$5 and a short amount of time on the FAA's website¹¹¹ to register their drones, which is well worth it: individuals who fail to register their drones can face stiff penalties, including a \$27,500 civil penalty, a \$250,000 criminal penalty, three years of jail time, or a combination of these.¹¹² These penalties were previously overturned by the United States Court of Appeals for the District of Columbia in the beginning of 2017, which cited the FAA Modernization and Reform Act of 2012 as allowing hobbyists to fly their drones with little oversight.¹¹³ More than 820,000 operators had

107. See Troy A. Rule, *Airspace in an Age of Drones*, 95 B.U. L. REV. 155, 163 (2015) (“Unfortunately, the United States will be unable to take full advantage of modern domestic drone technologies until federal, state, and local governments develop a more robust legal and regulatory structure to govern these high-tech devices.”).

108. Craig Whitlock, *Rogue Drones a Growing Nuisance Across the U.S.*, WASH. POST (Aug. 10, 2015), https://www.washingtonpost.com/world/national-security/how-rogue-drones-are-rapidly-becoming-a-national-nuisance/2015/08/10/9c05d63c-3f61-11e5-8d45-d815146f81fa_story.html.

109. See *Unmanned Aircraft Systems (UAS)/Drones*, PIEDMONT TRIAD INT'L AIRPORT, <https://flyfrompti.com/unmanned-aircraft-systems-uas-drones/> (last visited Apr. 7, 2018) (“The B4UFLY app provides model aircraft users with situational awareness and considers the user's current or planned location in relation to operational restrictions to derive a specific status indicator. The color- and shape-coded status indicators inform the user if model aircraft operation is prohibited, requires the user to take certain actions, or if there are no FAA operating restrictions other than flying safely.”).

110. Whitlock, *supra* note 108.

111. *FAADroneZone*, *supra* note 89.

112. Jacob Pramuk, *Unregistered Drone Users May Face Jail Time*, CNBC (Feb. 23, 2016, 2:17 PM), <https://www.cnbc.com/2016/02/23/unregistered-drone-users-may-face-jail-time.html>; Keith Wagstaff, *Fail to Register Your Drone? You Could Be Hit With \$27K Fine*, NBC NEWS (Dec. 15, 2015, 9:02 AM), <https://www.nbcnews.com/tech/innovation/fail-register-your-drone-you-could-be-hit-27k-fine-n481856>.

113. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 336(a), 126 Stat. 11, 77 (2012); e.g., *Taylor v. Huerta*, 856 F.3d 1089, 1091 (D.C. Cir. 2017).

registered their drones since December 2015—prior to when the federal court halted the required registration.¹¹⁴ John Taylor, a model aircraft enthusiast, filed suit against the FAA in January 2016, arguing that the FAA was prohibited from passing any rules regulating model aircraft operators. He further argued that model aircraft carriers would include non-commercial hobbyist drone operators.¹¹⁵ However, President Trump signed the 2018 National Defense Authorization Act into law in December 2017, which reinstated the registration requirement and the previously stated penalties for unregistered drones.¹¹⁶

F. Line of Sight Restrictions

Drones must be operated within a user's visual line of sight (VLOS), according to the FAA.¹¹⁷ VLOS means that drone operators must be able to visually see the drone without the aid of any optical device, such as binoculars, zoom lenses, or telescopes.¹¹⁸ In addition, VLOS prohibits the use of drones in dense fog, clouds, or at night when users are unable to maintain eye contact with the UAV.¹¹⁹

With the technology currently available, many UAVs are capable of flying well beyond a user's visual line of sight (BVLOS). However, without a waiver of the FAA regulation, it is prohibited in the United States to operate a drone BVLOS.¹²⁰ There are many potential commercial and government applications for drone use if owners were allowed to operate drones BVLOS, and a future increase in waiver applications is anticipated. Pilots using the first person view (FPV),

114. April Glaser, *Americans No Longer Have to Register Non-Commercial Drones with the FAA*, VOX (May 19, 2017, 1:54 PM), <https://www.recode.net/2017/5/19/15663436/us-drone-registration-rules-faa>.

115. Huerta, 856 F.3d at 1090. Judge Kavanaugh wrote that “[t]he Act codified the FAA’s longstanding hands-off approach to the regulation of model aircraft. Specifically, Section 336 of the Act, called the ‘Special Rule for Model Aircraft,’ provides that the FAA ‘may not promulgate any rule or regulation regarding a model aircraft.’” *Id.* at 1091 (quoting FAA Modernization and Reform Act, Pub. L. No. 112-95, § 336(a), 126 Stat. 11, 77 (2012)). The court determined that requiring hobbyist drone operators to register was a “rule or regulation” and that “statutory interpretation does not get much simpler. The Registration Rule is unlawful as applied to model aircraft.” *Id.* at 1092.

116. National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, § 1092(d), 131 Stat. 1283, 1611 (2017).

117. FAA Modernization and Reform Act, Pub. L. No. 112-95, § 336(c), 126 Stat. 11, 77–78 (2012); *see also* 14 C.F.R. § 107.31 (2019).

118. 14 C.F.R. § 107.31; *Summary of Small Unmanned Aircraft Rule (Part 107)*, *supra* note 101.

119. 14 C.F.R. §§ 107.29, .51; *Summary of Small Unmanned Aircraft Rule (Part 107)*, *supra* note 101.

120. *See Part 107 Waivers*, FED. AVIATION ADMIN., https://www.faa.gov/uas/commercial_operators/part_107_waivers/ (last modified Aug. 1, 2019, 2:14 PM).

which provides the UAV pilot a cockpit view via an onboard video camera to assist in navigation, are still operating a drone BVLOS and require the same FAA § 107.31 waiver.¹²¹

Extended visual line of sight (EVLOS) refers to a remote pilot in command (PIC) relying on remote observers of the UAV to keep the UAV in sight at all times once it is BVLOS of the PIC.¹²² Remote observers relay important flight information via radio or other communication to the PIC. Those wishing to operate a drone EVLOS must also obtain a waiver.¹²³

For the commercial use of drones to be successful, there must be a BVLOS system in place. Toward that end, Alphabet's Project Wing is working with the FAA and NASA to develop systems that could manage the air traffic control challenge of keeping drones from crashing into each other or other property.¹²⁴ The "unmanned aircraft systems Air Traffic Management" software (UTM) was successfully tested by six drones operating at the same time, simulating the pick-up and drop-off of packages.¹²⁵ The software makes adjustments to the flight path as the drones fly without the pilot needing to act.¹²⁶ No-fly zones, such as airports, could be added so that the UTM would know what areas the drones should avoid. While it was a successful test, a sample size of six drones is very small. An extensive amount of development is still needed, and the FAA expects that it will be at least 2019 before it can finalize collision-avoidance standards.¹²⁷

Ground-based and airborne "sense and avoid" technologies, which can enable drones to sense objects in their path and change course in order to avoid collisions, are safety features under development that could help with BVLOS flights.¹²⁸ Other programs that are designed to automatically send drones back to the ground safely if they are disconnected from the remote operators' signals, such as "lost-link" or

121. *Summary of Small Unmanned Aircraft Rule (Part 107)*, *supra* note 101.

122. ALLISON FERGUSON, ENABLING BEYOND LINE OF SIGHT WITH THE FAA PATHFINDER PROGRAM: EXTENDED VISUAL LINE OF SIGHT 1 (2017), https://www.astm.org/COMMIT/XPO17/Paper_Ferguson.pdf.

123. *See Part 107 Waivers*, *supra* note 120.

124. Jamie Condliffe, *Alphabet's New Air Traffic Control System Steers Drones Away from Peril*, MIT TECH. REV. (June 7, 2017), <https://www.technologyreview.com/s/608050/alphabets-new-air-traffic-control-system-steers-drones-away-from-peril/>.

125. *Id.*

126. *Id.*

127. *Id.*

128. *See* Thomas Black, *Amazon's Drone Dream Sets Off Race to Build Better Sensor*, BLOOMBERG (June 7, 2014, 12:01 AM), <https://www.bloomberg.com/news/articles/2014-06-06/amazon-s-drone-dream-sets-off-race-to-build-better-sensor> [http://perma.cc/3K36-YLSS] ("Sense and avoid is one of the biggest opportunities in the industry . . .").

“return-to-base,” would be valuable standard features for small drones.¹²⁹ Another safety concern is that one could hack into a drone’s signals during flight to send rogue signals and take control of the drone, intentionally directing it to cause harm. An anti-hacking system to prevent such signal interception would be a recommended requirement.¹³⁰

One challenge for landowners trying to report drone activity is being able to sufficiently identify the drone for authorities to be able to track down the owner. Perhaps the FAA could require GPS software to be installed in the drones so that they could be tracked. However, each of these proposed systems would cost time and money to develop while also increasing the cost of drones. Some might argue that increased cost is a good thing because it could potentially reduce the number of drones in the air. However, if drones are going to be useful to businesses, then cost control is important.

The FAA is developing the Low Altitude Authorization and Notification Capability system (LAANC) to give commercial operators pre-approved flight zones and maximum altitudes for operating UAVs near airports rather than requiring a waiver.¹³¹ As of 2018, the system is still in beta form, but the list of participating facilities is growing.¹³² The goals of LAANC would be to automate the waiver application process, reduce the wait time for approvals, and give recreational drone pilots a way to notify airport air traffic control when they will fly near an airport.¹³³ While LAANC will provide more access to airspace, it is not an unmanned traffic management system and is not intended to be.¹³⁴

129. See WENDIE KELLINGTON, LAND USE INST., UNMANNED AIR SYSTEMS AND REGULATING NAVIGABLE AIRSPACE 11 (2013), <https://perma.cc/G8FD-RLEY> (“UAVs often include programmed maneuvers to be automatically deployed if a command and control link is disrupted . . .”).

130. See, e.g., Joshua Turner & Sara Baxenberg, *NASCAR Drone Countermeasures May Be Illegal*, LAW360 (Apr. 18, 2018, 4:55 PM), <https://www.law360.com/articles/1034908/nascar-drone-countermeasures-may-be-illegal>.

131. Wilson, *supra* note 100.

132. *FAA Facilities Participating in LAANC*, FED. AVIATION ADMIN., https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/airports_participating_in_laanc/ (last updated Aug. 26, 2019).

133. Wilson, *supra* note 100.

134. See *id.*

III. AIRSPACE TRESPASS

A. *Airspace Trespass by Something Other than Drones*

As the use of drones increases, trespass litigation by landowners is likely to increase. However, to date, there have been few drone cases to serve as precedent.¹³⁵ In order for the courts to decide these new cases, they will need to look at parallel trespass cases for guidance on the extent to which intrusion into the airspace of another constitutes trespass.¹³⁶ For example, in an analogous case in 1993, the Wagners cut down tree limbs that originated from trees on the Joneses' property.¹³⁷ The limbs were hanging over a fence that separated property boundaries and onto the Wagners' property.¹³⁸ In other words, the limbs were encroaching on the Wagners' airspace. The Joneses sought damages, claiming that the Wagners had no right to trim the tree limbs and that the limbs did not trespass because they did not cause any harm.¹³⁹ The Pennsylvania Superior Court found that the issue of whether one could utilize self-help by cutting down overhanging limbs had been determined several times before¹⁴⁰ and was not limited solely to an interest in land:

But the interest in exclusive possession is not limited to the surfaces; it extends above and below. There is a property right in the air space above the land, which may be invaded by overhanging structures, or telephone wires, by thrusting an arm above the boundary line, or by shooting across the land, even though the bullets do not fall upon it.¹⁴¹

The court emphasized that a landowner can enforce his right to freely enjoy exclusive use of his property without any physical harm or damage present.¹⁴² In this context, landowners have a right to enjoy the land they

135. Zack Kurzhals, *Drones, Damages, and Property Rights*, U. CIN. L. REV. BLOG (Nov. 1, 2017), <https://uclawreview.org/2017/11/01/drones-damages-and-property-rights/>.

136. See RESTATEMENT (SECOND) OF TORTS § 159(2) (AM. LAW INST. 1965) ("Flight by 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.").

137. *Jones v. Wagner*, 624 A.2d 166, 167 (Pa. Super. Ct. 1993).

138. *Id.*

139. *Id.* ("[The Joneses] claim that [the Wagners] are liable to them at law since [the Wagners], having suffered no appreciable damage by the overhanging branches, are not entitled to exercise a self-help remedy by trimming the trees.>").

140. *Id.*

141. *Id.* at 169 (citations omitted).

142. *Id.*; see also JACQUELINE P. HAND & JAMES CHARLES SMITH, NEIGHBORING PROPERTY OWNERS § 5:3, at 114 (1988) ("If a building is constructed so that part of it projects across the boundary line at a point above the surface, trespass is available. An example would be eaves of a

rightfully possess, free from any sort of airspace intrusion, even if the tree limbs do not cause any property damage or bodily injury.¹⁴³ The court also noted that “continued presence of a structure, chattel, or other thing which the actor has tortiously placed there, whether or not the actor has the ability to remove it”¹⁴⁴ is a continuing trespass, which would permit the Wagners to even cut the branches again when they regrow. “An actor places branches ‘tortiously’ on another’s property when he is subject to liability in tort, that is, when he is trespassing onto another’s property.”¹⁴⁵

In another analogous case, a landowner successfully argued that his neighbor trespassed in breaking down a fence surrounding the landowner’s property and building a barn with eaves that extended over the owner’s property.¹⁴⁶ Another example of a parallel case involved defendants who ran clothes reels with laundry onto plaintiffs’ property and actually interfered with plaintiff’s use of the premises.¹⁴⁷ While initially there was permission for the reels, the plaintiff subsequently revoked it.¹⁴⁸ Thereafter, “each extension of the reels over the plaintiffs’ land, contrary to their wishes, was an unlawful invasion of the legal rights of the plaintiffs and constituted a separate trespass.”¹⁴⁹ One can also look to *Wandsworth Board of Works v. United Telephone Co.*, an old English case that is often cited when plaintiffs claim that their airspace rights have been infringed.¹⁵⁰ In *Wandsworth*, an unauthorized telephone wire the defendant had installed hung over the property lines and into the plaintiff’s airspace.¹⁵¹ The court found the presence of the telephone wire

roof that overhang a neighbor’s land. Similarly, utility wires cannot be strung across land without the consent of its owner, even though none of the poles or standards are located on the owner’s surface.”).

143. *Jones v. Wagner*, 624 A.2d 166, 169 (Pa. Super. Ct. 1993) (“Thus, there is no question that a branch overhanging a landowner’s property line is a technical trespass which he may alleviate by exercising self-help, as did appellees here. They were entitled to trim the encroaching branches without regard to the degree of physical harm done to their property. The redressable harm caused by the trees is that of the trespass onto appellees’ property, not physical damage done to their land.”). Contrast that, though, with nuisance. While the court said that “[i]t may be understood that any erection upon one man’s land, that projects over the land of another, as well as any tree whose branches thus project, doing actual damage, or anything that interferes with the rights of an adjoining landowner, is an actionable nuisance,” it acknowledged that some courts had found that “appreciable damage must be shown in order to give overhanging branches the character of nuisance.” *Id.* at 168–69.

144. *Id.* at 170 (citing RESTATEMENT (SECOND) OF TORTS § 161(1) (AM. LAW INST. 1965)).

145. *Id.* (citing RESTATEMENT (SECOND) OF TORTS § 161 cmt. a (AM. LAW INST. 1965)).

146. *Smith v. Smith*, 110 Mass. 302, 303–04 (Mass. 1872).

147. *Scioscia v. Iovieno*, 63 N.E.2d 898, 898–99 (Conn. Super. Ct. 1945).

148. *Id.* at 899.

149. *Id.*

150. *See generally* *Wandsworth Bd. of Works v. United Tel. Co.* [1884], 13 QBD 904 (Eng.).

151. *Id.* at 905.

to be a trespass and ruled in favor of the plaintiff.¹⁵² It was not material to the case whether or not the plaintiff would or could use the airspace.¹⁵³ Likewise, UAV operators could find themselves liable for trespassing on private property without the landowners having to prove whether they would actually use the property or suffer harm.

Similar to *Wandsworth*, the court in *Didow v. Alberta Power Ltd.* ruled in favor of the plaintiff, who sued the defendant for trespass, because the defendant's power lines hung above the plaintiff's property.¹⁵⁴ What is unclear—and again presents a challenge for drone operators—is determining at what specific height an airspace intrusion constitutes a trespass. In *Didow*, the contested power lines were fifty feet above the surface and protruded six feet onto Didow's land.¹⁵⁵ The court found that it could not literally apply the maxim that whoever owned the land owned the sky up to the heavens.¹⁵⁶ However, the court did find that interfering with an owner's airspace by encroaching upon the potential or actual use of the airspace constitutes trespass.¹⁵⁷ In both *Didow* and *United States v. Causby*, the courts' ambiguous language leaves UAV operators in a tricky situation when flying over private property.¹⁵⁸ Neither case specified a specific limit to private airspace, but rather that trespass includes anything that interferes with the enjoyment or use of private land.¹⁵⁹

The use of cranes has helped allow areas all over the United States, namely urban communities, to explode in size. A crane's jib, the long extended arm, needs to swing freely in the wind when not in use to help it stabilize, so many developers seek consent of adjoining owners to allow the jib to enter private airspace to avoid a trespass claim.¹⁶⁰ In *Whitney National Bank of New Orleans v. Poydras Center Associates*, no such consent was obtained.¹⁶¹ Whitney obtained a temporary restraining order (TRO) enjoining defendants "from trespassing on either the surface, subsurface or air rights" of Whitney's property by the "use of cranes, dust or any other instrumentality or substance intruding on, under or over" Whitney's property, arguing that using a crane over neighbor's property

152. *Id.* at 907–08.

153. *See id.* at 908.

154. *Didow v. Alberta Power Ltd.* (1988), 88 A.R. 250 (Can.).

155. *Id.*

156. *Id.*

157. *Id.*

158. *See id.*; *U.S. v. Causby*, 328 U.S. 256, 264–65 (1946).

159. *Didow*, 88 A.R. 250 (Can.); *Causby*, 328 U.S. at 265–66.

160. Jesse S. Ishikawa, *Tower Cranes, Trespass, and Temporary Airspace Use Agreements*, *PROB. & PROP.*, Jan.–Feb. 2006, at 63, 65.

161. *Whitney Nat'l Bank of New Orleans v. Poydras Ctr. Assocs.*, 468 So. 2d 1246, 1247 (La. Ct. App. 1985).

would be trespassing.¹⁶² Poydras sought to dissolve the TRO and multiple hearings followed.¹⁶³ By the time the court was ready to rule, construction had been completed, so the court refused to issue an injunction to prevent activity that had already been completed.¹⁶⁴ Many developers in recent years have sought temporary easements or license agreements with neighboring property owners while completing construction to keep from inadvertently trespassing.¹⁶⁵ Could this be the route UAV owners will be required to take in the future to prevent trespasses?

The use of firearms and the paths of their bullets give another good example for courts and drone operators to reference when dealing with this complex issue. In the 1925 Montana Supreme Court case *Herrin v. Sutherland*, the plaintiff sued the defendant for trespass after the defendant fired a shotgun and the shotgun shells traveled over the plaintiff's private property.¹⁶⁶ The plaintiff argued that the shots "interfered with 'the quiet, undisturbed, peaceful enjoyment' of the plaintiff" at his dwelling-house, ranch, and property.¹⁶⁷ The court sided with the plaintiff and affirmed that the bullets constituted a trespass that disturbed the quiet and peaceful use of the land.¹⁶⁸ In addition, the court said that there was a clear danger with a shotgun being fired over the plaintiff's property even without actual damages.¹⁶⁹

The court's decision could cause trouble for drone operators because there is no need for actual damages from the aerial trespass, only the possibility of danger. Drones are mechanical objects that sometimes fail. Even if a capable drone operator were allowed to fly over private property, a drone can still possibly run out of battery or cease to operate for any number of reasons, which could cause it to fall out of the sky and injure an unsuspecting individual. Therefore, the language of the court's opinion issued in *Herrin v. Sutherland* does not give reassurance to drone operators but only complicates the issue.

An old case about horses in England from the late 1800s provides another example of the challenges that courts face. In *Ellis v. Loftus Iron Co.*, the court found the defendant liable for trespass onto the land of his neighbor when the defendant's horse stuck his head through a wire fence and bit the plaintiff's horse.¹⁷⁰ The court's decision was important

162. *Id.*

163. *Id.*

164. *Id.* at 1249.

165. Ishikawa, *supra* note 160, at 65.

166. *Herrin v. Sutherland*, 241 P.2d 328, 329 (Mont. 1925).

167. *Id.* at 331–32.

168. *Id.*

169. *Id.* at 332.

170. *Ellis v. Loftus Iron Co.* [1874], 10 LRCP 10 (Eng.).

because it determined that the horse engaged in a trespass although it never physically touched the ground of neighboring land.¹⁷¹ In addition, although the horse caused physical damage to the plaintiff's property in this specific case, the court found that merely an intrusion that affects the enjoyment of private property also constitutes a trespass.¹⁷² The presiding judge in the case, Lord Coleridge, had this to say in his decision:

It is clear that, in determining the question of trespass or no trespass, the court cannot measure the amount of the alleged trespass; if the defendant places a part of his foot on the plaintiff's land unlawfully, it is in law as much a trespass as if he had walked half a mile on it.¹⁷³

As evidenced by this statement, Lord Coleridge believed that a trespass was the same in the court's eye no matter if by a few inches or a few thousand feet. This idea presents a major issue for drone operators because, under this view, if a drone crosses over into private property by only a foot, the operators could be held liable for trespass. The courts would find it extremely difficult to determine the precise location of a drone in relation to the boundaries of private property to determine whether a trespass occurred. Such difficulty may lead the court to favor the landowner, erring on the side of trespass.

B. *Airspace Trespass by Drones*

The recent federal court case *Boggs v. Merideth* best highlights the legal difficulties faced by UAV operators.¹⁷⁴ The plaintiff was operating his drone in uncontrolled and navigable Class G airspace above the defendant's property when the defendant shot down the drone with a shotgun.¹⁷⁵ The plaintiff argued that he was operating the drone in the "navigable airspace" and high enough not to constitute a trespass, but the defendant claimed that the drone was being operated on her property.¹⁷⁶ The judge dismissed the lawsuit, and while the decision appears to be a win for landowners, the issue is far from resolved.¹⁷⁷

171. *Id.* at 12.

172. *Id.* at 13.

173. *Id.* at 12.

174. *Boggs v. Merideth*, No. 3:16-cv-00006-TBR, 2017 U.S. Dist. LEXIS 40302 (W.D. Ky. Mar. 21, 2017); *see also* Fieldstadt, *supra* note 5.

175. *Boggs*, 2017 U.S. Dist. LEXIS 40302, at *1–2.

176. *Id.*

177. *Id.* at *24.

The plaintiff then brought his case to federal court because he claimed that the drone in question was subject to the FAA's federal regulation.¹⁷⁸ However, Judge Russell concluded the following:

But even if Boggs is correct that his unmanned aircraft *is* subject to federal regulation, as the Court noted above, the fact remains that the FAA has not sought to enforce any such regulations in this case. Moreover, FAA regulations, at most, would constitute ancillary issues in this case, in which the heart of Boggs' claim is one for damage to his unmanned aircraft under Kentucky state law.¹⁷⁹

Thus, the court does not completely clear the defendant of any wrongdoing, but states that the issue should be taken up in a state court as opposed to a federal court.¹⁸⁰ Both drone operators and landowners need to take this decision with caution, as concrete aerial property boundaries are still far from being clarified.

IV. STATE AND LOCAL REGULATION OF DRONES

A. *State Regulation of Drones*

If state tort law is going to apply to trespass by drones, then states will want to exercise some power over drone regulation within their boundaries. This is not a question of federal preemption, but rather additional state regulation over its uncontrolled airspace. The United States Department of Transportation (DOT) recently granted ten special licenses to UAS projects backed by state and local governments.¹⁸¹ The DOT's Unmanned Aircraft Systems Integration Pilot Program's goal is to "foster a meaningful dialogue on the balance between local and national interests related to UAS integration, and provide actionable information to the USDOT on expanded and universal integration of UAS into the national airspace system."¹⁸² However, there is some concern

178. *See id.* at *12.

179. *Id.* at *14.

180. *Id.* at *24.

181. Chiem, *supra* note 38 (reporting that Alaska, California, Florida, Kansas, Nevada, North Carolina, North Dakota, Oklahoma, Tennessee, and Virginia will participate in the DOT's Unmanned Aircraft Systems Integration Pilot Program to test commercial drone operations that would typically require waivers, including package delivery and nighttime flights). Specifically, a 1,500-pound UAV will monitor mosquitoes in Florida, and Flirtey, a medical equipment startup, will fly drones with emergency medical equipment to heart-attack victims in Nevada. David Shepardson & Jeffrey Dastin, *U.S. Drone Program Taps Apple, Passes Over Amazon, China's DJI*, REUTERS (May 9, 2018, 1:27 PM), <https://www.reuters.com/article/us-usa-drones-companies/us-drone-program-taps-alphabet-passes-over-amazon-chinas-dji-idUSKBN1IA2WC>.

182. Chiem, *supra* note 38.

about state regulations attempting to dilute federal regulations, particularly Part 107.¹⁸³

Congress gave the FAA the authority to regulate aviation safety, the scope of which includes drone operations, but states are implementing rules to regulate drone-related concerns such as property rights, liability, and privacy.¹⁸⁴ Regulation of airspace below navigable airspace should belong to states because state tort law will be implicated. States regulate drivers' licenses, so why not regulate drone licenses?¹⁸⁵ While the FAA may regulate airspace,¹⁸⁶ state and local governments have some power to regulate the use of airspace, and therefore, the use of that airspace by drones. Amanda Essex, a policy associate for the National Conference of State Legislatures, commented: "I wouldn't necessarily say there is one state doing it better than the others. They're all kind of taking their own approaches as to what they think is going to work for their state and what is best in their situation."¹⁸⁷

In the 2017 legislative session, thirty-eight states considered UAS legislation, resulting in eighteen of those states passing twenty-four pieces of legislation.¹⁸⁸ Three states adopted resolutions to address UAS legislation in 2018.¹⁸⁹ Alaska has a Task Force on UAS, North Dakota supports the development of the UAS industry, and Utah supports the building of a NASA drone testing facility and Command Control Center in Tooele County, Utah.¹⁹⁰ Utah also passed legislation extending criminal trespass to drones and prohibiting the disturbance of livestock

183. See *Singer v. City of Newton*, No. CV 17-10071, 2017 WL 4176477 (D. Mass. Sept. 21, 2017); see generally Nicholas Cody, Note, *Flight and Federalism: Federal Preemption of State and Local Drone Laws*, 93 WASH. L. REV. 1495 (2018).

184. See Eyragon Eidam, *Report: Drone Legislation a Priority for States Across the U.S.*, GOV'T TECH. (July 11, 2016), <http://www.govtech.com/policy/Report-Drone-Legislation-a-Priority-for-States-Across-the-US.html>.

185. Rule, *supra* note 107, at 203 ("Through drone operator license tests, periodic safety inspections, liability insurance criteria, and related means, such licensing systems could do a great deal to promote drone safety and to ensure that drone users are familiar with laws relating to the devices.").

186. See Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 731.

187. Eidam, *supra* note 184.

188. *Current Unmanned Aircraft State Law Landscape*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 10, 2018), <http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx>.

189. *Id.*

190. *Id.*

with drones.¹⁹¹ Virginia made it a misdemeanor for a UAS to trespass for the purpose of spying.¹⁹²

Austin Haughwout, a nineteen-year-old, posted YouTube videos of a drone using a flamethrower to roast a turkey¹⁹³ and another of a drone holding and shooting a gun.¹⁹⁴ The FAA has been investigating, but Haughwout and his father argue that the FAA is exceeding its authority because drones are models, not aircraft, and because his videos are of a backyard hobby, not commercial use.¹⁹⁵ Mario Cerame, Haughwout's attorney, argued that "[c]onstruing small civilian drones as aircraft is not consonant with the history and policy purpose of the FAA. It was about airplanes, helicopters, and blimps, and the accoutrements that accompany them."¹⁹⁶ Those incidents led to a proposed Connecticut law prohibiting the remote control of a deadly weapon.¹⁹⁷

In California, a property owner's rights in the airspace over his land include rights to the "free or occupied space [above the property] for an indefinite distance upwards . . . subject to limitations upon the use of airspace imposed . . . by law."¹⁹⁸ In September 2015—following several incidents between firefighters and drones—California state legislators

191. UTAH CODE ANN. § 76-9-308 (LexisNexis 2019) ("[A] person is guilty of harassment of livestock if the person intentionally, knowingly, or recklessly chases, with the intent of causing distress, or harms livestock through the use of . . . an unmanned aircraft system."); *see also* § 76-6-206(2)(a) ("A person is guilty of criminal trespass if . . . the person . . . causes an unmanned aircraft to enter and remain unlawfully over property . . .").

192. VA. CODE ANN. § 18.2-130.1 (2017) ("It is unlawful for any person to knowingly and intentionally cause an electronic device to enter the property of another to secretly or furtively peep or spy . . . into . . . a dwelling . . . is a Class 1 misdemeanor.")

193. Hogwit, *Roasting the Holiday Turkey*, YOUTUBE (Dec. 7, 2015), <https://www.youtube.com/watch?v=lmD3rXUR1Tw> (listing over 700,000 views as of May 14, 2019).

194. Hogwit, *Flying Gun*, YOUTUBE (July 10, 2015), <https://www.youtube.com/watch?v=xqHrTivFFIs> (listing over four million views as of May 14, 2019).

195. Edmund H. Mahony, *Drone-Flying Teen and His Dad Go to Court to Fight FAA Investigation*, HARTFORD COURANT (July 6, 2016, 9:15 PM), <http://www.courant.com/news/connecticut/hc-drone-boy-0707-20160706-story.html>.

196. *Id.*

197. H.R. 7260, 2017 Leg., Gen. Assemb., Jan. Sess. (Conn. 2017), <https://www.cga.ct.gov/2017/TOB/h/2017HB-07260-R00-HB.htm> ("Except as otherwise provided by law, no person . . . shall operate or use any computer software or other technology, including, but not limited to, an unmanned aerial vehicle, that allows such person, when not physically present, to release tear gas or any like or similar deleterious agent or to remotely control a deadly weapon, as defined in section 53a-3 of the general statutes, or an explosive or incendiary device, as defined in section 53-206b of the general statutes."); Miriam McNabb, *Connecticut Decides Against "Weaponized" Drones for Law Enforcement*, DRONELIFE (May 2, 2017), <https://dronelife.com/2017/05/02/connecticut-decides-weaponized-drones-law-enforcement/> (reporting that Connecticut's House of Representatives did not take action on Connecticut House Bill 7260).

198. CAL. CIV. CODE § 659 (West 2019).

passed a bill¹⁹⁹ granting immunity to emergency responders who damage a drone that gets in their way.²⁰⁰ In one case, a drone interfered with helicopters fighting a major fire in Northern California, causing a delay of ten minutes.²⁰¹ The pilot of the drone was given a citation, but he commented that he did not know that flying his drone near the airport was illegal.²⁰² However, in California, such interference is a misdemeanor.²⁰³

In 2013, Oregon was one of the early states to enact a statute creating a civil claim for drone trespass.²⁰⁴ The statute, as enacted, allowed real property owners to bring claims against anyone who flew a drone over their property below 400 feet, but not for the first such flight.²⁰⁵ The property owner must have first asked the pilot not to fly over the property, and then if the pilot flies the drone a second time, the property owner can bring a trespass claim.²⁰⁶ In such a case, prevailing plaintiffs can recover treble damages for any injuries to persons or property caused by the unwanted drone and, in some cases, attorney fees.²⁰⁷

199. *Id.* § 43.101(a) (West 2019) (“An emergency responder shall not be liable for any damage to an unmanned aircraft or unmanned aircraft system, if that damage was caused while the emergency responder was providing, and the unmanned aircraft or unmanned aircraft system was interfering with, the operation, support, or enabling of the emergency services listed in Section 853 of the Government Code.”).

200. Whitlock, *supra* note 108 (reporting that in California, drones interfered with firefighters’ efforts to battle wildfires and that in New York, firefighters used their water hoses to knock down a drone that had been filming them as they battled a house blaze).

201. Press Release, Petaluma Police Dep’t, 24 Year Old Petaluma Resident Cited for Flying a Drone over the Petaluma Airport Halting Cal. Fire Helicopters (Oct. 15, 2017, 10:10 PM), <http://www.nixle.us/9MZ35> (stating that 24-year-old Nestor Rodriguez received a citation for Impeding Emergency Personnel for flying a drone over the airport being used by the firefighting helicopters).

202. *Id.*

203. CAL. PEN. CODE § 402 (West 2019) (“It is unlawful to knowingly, intentionally, or recklessly operate an unmanned aircraft or unmanned aircraft system in a manner that prevents or delays the extinguishment of a fire, or in any way interferes with the efforts of firefighters to control, contain, or extinguish a fire, including, but not limited to, efforts to control, contain, or extinguish the fire from the air. A violation of this section is punishable by imprisonment in a county jail not to exceed six months, by a fine not to exceed five thousand dollars (\$5,000), or by both that imprisonment and fine.”).

204. OR. REV. STAT. § 837.380 (2013) (amended 2016).

205. *Id.* § 837.308(1)(a).

206. *Id.* § 837.308(1)(b).

207. *Id.* § 837.380(3)–(4).

B. Local Regulation

1. Community Regulation

In addition to state-wide regulations, states often delegate regulation of local community activities.²⁰⁸ Municipalities regulate many activities that impact landowners and neighbors, ranging from the lighting of fireworks²⁰⁹ to the raising of backyard chickens.²¹⁰ “In early 2013, Charlottesville, Virginia became the first city to pass an anti-drone resolution. And [Texas] House Bill 912, also known as the Texas Privacy Act, makes using drones for surveillance a crime.”²¹¹

In Honolulu, Hawaii, Skysign International, Inc. had an FAA waiver certificate permitting its helicopters to carry lighted advertising signs beneath their fuselages.²¹² That federal certificate specifically provided: “The operator, by exercising the privilege of this waiver, understands all local laws and ordinances relating to aerial signs, and accepts responsibility for all actions and consequences associated with such operations.”²¹³ Both the city and county of Honolulu bar the use of aircraft to display “any sign or advertising device.”²¹⁴ According to the Ninth Circuit Court of Appeals, the Honolulu aerial signage ordinance specifically targeted navigable airspace as “an area where there has been a history of significant federal presence.”²¹⁵ Skysign tried to argue that the federal regulation of airspace preempted the state regulations, but

208. See, e.g., Richard Briffault, *Home Rule for the Twenty-First Century*, 36 URB. LAW. 253, 258–59 (2004) (“If all political decisions were centralized at the state level, it would be difficult to vary these policies to take into account varying local needs, circumstances, and preferences Home rule permits cities and suburbs, liberal communities and conservative communities, ethnically diverse and ethnically homogeneous settings, to adopt policies that reflect their differing values and conditions. It thus increases the likelihood that people will be happy with their government.”).

209. See 7A EUGENE MCQUILLIN, *THE LAW OF MUNICIPAL CORPORATIONS* § 24:471 (3d ed. 2014) (“Fireworks ordinances enacted by municipalities are ordinarily sustained as a valid exercise of their police power.” (citation omitted)).

210. See Jaime Bouvier, *Illegal Fowl: A Survey of Municipal Laws Relating to Backyard Poultry and a Model Ordinance for Regulating City Chickens*, 42 ENVTL. L. REP. 10888, 10903–17 (2012) (surveying residential chicken-raising ordinances in the 100 most populous United States cities and determining that backyard chicken raising is permitted under certain conditions in residential areas within most of the nation’s largest cities).

211. Sterbenz, *supra* note 25.

212. *Skysign Int’l, Inc. v. City and Cty. of Honolulu*, 276 F.3d 1109, 1113 (9th Cir. 2002).

213. *Id.*

214. HONOLULU, HAW., REV. ORDINANCES § 40-6.1 (1990 & Supp. 1996).

215. *Skysign Int’l*, 276 F.3d at 1116 (quoting *United States v. Locke*, 529 U.S. 89, 108 (2000)).

since the certificates specifically referenced state and local law, that argument ultimately failed.²¹⁶

Some states focus on the purpose of the drone flight rather than the flight itself. In Tennessee, it is a crime to use “a drone with the intent to conduct video surveillance of private citizens who are lawfully hunting or fishing without obtaining the written consent of the persons being surveilled prior to conducting the surveillance.”²¹⁷ Similarly, in Barstow, California, a UAS cannot be operated “in a manner that harasses, startles, or annoys pedestrians or vehicles.”²¹⁸

2. Prevention of Drones

In addition to possible civil liability for unwelcome drone usage, some landowners are taking matters into their own hands. For example, NASCAR did not want drones flying over the Texas World Speedway during a race in Fort Worth, Texas, so it contracted with DroneShield to track and interdict unauthorized drones.²¹⁹ DroneShield claims that it coordinated with state and local Texas authorities to implement its solution to use a high-powered directional radio jammer called a “DroneGun” to protect the race.²²⁰ However, the FCC warned that “it is illegal to use a cell phone jammer or any other type of device that blocks, jams or interferes with authorized communications. This prohibition extends to every entity that does not hold a federal authorization, including state and local law enforcement agencies.”²²¹ In addition to prohibiting signal jamming, there are additional legal issues associated with attempts to intercept and disable aircraft, including unmanned aircraft. Section 32(a)(1) of Title 18 provides that, “[w]hoever willfully . . . sets fire to, damages, destroys, disables, or wrecks any aircraft” is guilty of a federal felony.²²² That provision has not yet been used in the context of drones, but it could be applied in the future. Typically, drone countermeasures, including signal jammers, are only permitted to be used by the United States Department of Defense to protect military installations.²²³

216. *Id.* at 1114.

217. TENN. CODE ANN. § 70-4-302(a)(6) (2014).

218. BARSTOW, CAL. CODE OF ORDINANCES § 9.66.020(b) (2017).

219. Turner & Baxenberg, *supra* note 130.

220. *Id.*

221. 47 U.S.C. § 333 (2018) (“No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this chapter or operated by the United States Government.”).

222. 18 U.S.C. § 32(a)(1) (2018).

224. *See* Turner & Baxenberg, *supra* note 130.

Another form of drone defense is the drone catcher, invented by Mo Rastgaar, an associate professor of mechanical engineering at Michigan Technological University.²²⁴ His theory was that even if there were a legitimate security interest to disable a drone, like threatening a military installation or the White House, shooting it down could create additional problems, so he devised a way to catch the drone with a net and take it safely to the ground.²²⁵

3. University Regulation

Some universities are prohibiting the use of drones on campus. For example, the University of Notre Dame's Standards of Conduct state that "the University prohibits any student from using Unmanned Aerial Systems (UAS), or Drones, on campus."²²⁶ Similarly, Janielle Tchakerian, Assistant Vice President for Student Affairs for Saint Mary's College said, "Since Saint Mary's College is in the flight path to the South Bend airport, we wanted to inform our students that for the safety of the manned aircrafts flying above our campus that drones are prohibited."²²⁷

V. ADDITIONAL TORTS

A. Nuisance

One might argue that interference by a drone is closer to a nuisance than a trespass. A nuisance claim requires a person or object to interfere with the landowner's ability to use and enjoy his or her land.²²⁸ However,

224. Marcia Goodrich, *Drone Catcher: "Robotic Falcon" Can Capture, Retrieve Renegade Drones*, MICH. TECH (Jan. 7, 2016, 10:17 AM), <http://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html>.

225. *Id.* ("What makes this unique is that the net is attached to our catcher, so you can retrieve the rogue drone or drop it in a designated, secure area. It's like robotic falconry.")

226. *Prohibition on Drones and Unmanned Aerial Systems*, U. NOTRE DAME, <http://dulac.nd.edu/community-standards/standards/drones/> (last visited Oct. 25, 2018); *Game Day Policies*, U. NOTRE DAME (Oct. 29, 2016), <https://gameday.nd.edu/news/stadium-bag-policy/> ("The Federal Aviation Administration (FAA) prohibits the operation of any UAS within a 5 mile radius of an airport. Given the University's proximity to the South Bend International Airport (SBN), any use of UAS on campus is strictly prohibited."). However, the University of Notre Dame Wireless Institute is working with the city of South Bend to test advanced wireless research using a drone. Erin Blasko, *South Bend and Notre Dame Demonstrate Next-Gen Wireless*, SOUTH BEND TRIB. (Mar. 21, 2017), https://www.southbendtribune.com/news/local/south-bend-and-notre-dame-demonstrate-next-gen-wireless/article_cf50c778-c15c-5d41-91aa-c60b696d2872.html.

227. Nicole Caratas, *Saint Mary's Bans 'Hoverboards' and Drones*, OBSERVER (Jan. 15, 2016), <http://ndsmcobserver.com/2016/01/hoverboards-and-drones-banned-at-smc/>.

228. *Martin v. Reynolds Metals Co.*, 342 P.2d 790, 795 (Or. 1959); *see also* Int'l Union of Painters & Allied Trades Dist. Council 15 Local 159 v. Great Wash Park, LLC, No. 67453, 2016 WL 4165919, at *8 (Nev. Ct. App. July 29, 2016) (Tao, J., concurring) (pointing out that nuisance requires an inquiry "into whether the intensity, duration, or other qualities" of the objectionable

a nuisance claim can succeed even if the interference flew over the neighbor's adjoining land, but not directly into plaintiff's airspace, as long as the flight constitutes a substantial and unreasonable interference with the use and enjoyment of the land.²²⁹ UAVs present a threat as both a trespass and a nuisance with their ability to physically invade private property as well as interfering with the enjoyment of one's private property.²³⁰ As noted in *Hinman*, however, the rights to the use of one's land may not be fixed.²³¹

According to Robert L. Ellis,²³² “[a] century ago, a court expressed what might be called the ‘noises of progress’ principle when dismissing a property owner’s nuisance claim against a railroad: ‘A material amount of noise is produced . . . by modern civilization.’”²³³ He went on to point out that “[i]n another early case, the court refused to enjoin a business from staying open late and attracting traffic, pointing out that the recent appearance of automobiles on the roads, including at night, had become normal ‘but would some years ago have been considered a nuisance.’”²³⁴ It is unclear whether courts will apply the “noises of progress” principle to drone nuisance lawsuits or if they will allow drone nuisance claimants

interference were unreasonable or excessive, whereas there is no such analysis in a trespass claim—either there was an interference or there was not). *See generally* RESTATEMENT (SECOND) OF TORTS § 821D (AM. LAW INST. 1979) (distinguishing trespass as an interference with a property owner’s right to exclusive possession of a property from a nuisance, which is an interference with the owner’s use or enjoyment of the property).

229. ALISSA M. DOLAN & RICHARD M. THOMPSON II, CONG. RES. SERV., INTEGRATION OF DRONES INTO DOMESTIC AIRSPACE: SELECTED LEGAL ISSUES 11 (Apr. 4, 2013), <https://fas.org/sgp/crs/natsec/R42940.pdf>.

230. A drone might also be considered a projectile, which has also been held to be actionable trespass. *See* RESTATEMENT (SECOND) OF TORTS § 158 cmt. i (“[I]n the absence of the possessor’s consent or other privilege to do so, it is an actionable trespass to throw rubbish on another’s land . . . or to fire projectiles . . . through the air above it, even though no harm is done to the land or to the possessor’s enjoyment of it.”); *see also* Eugene Volokh, *Is Projecting a Message onto the Wall of a Building a Trespass? A Nuisance?*, WASH. POST (Aug. 17, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/08/17/is-projecting-a-message-onto-the-wall-of-a-building-a-trespass-a-nuisance/?utm_term=.92044cd016d5.

231. *Hinman v. Pac. Air Transp.*, 84 F.2d 755, 758 (9th Cir. 1936) (“We own so much of the space above the ground as we can occupy or make use of, in connection with the enjoyment of our land. This right is not fixed. It varies with our varying needs and is coextensive with them. The owner of land owns as much of the space above him as he uses, but only so long as he uses it.”); *see also* *Geller v. Brownstone Condo. Ass’n*, 402 N.E.2d 807, 809 (Ill. App. Ct. 1980) (“And to constitute an actionable trespass, an intrusion has to be such as to subtract from the owner’s use of the property.”).

232. Robert L. Ellis, *Mastering Small Unmanned Aircraft Systems Regulations*, ROSSDALE CLE 6 (Sept. 14, 2017).

233. *Id.* (citing *Dean v. S. Ry. Co. in Mississippi*, 73 So. 55, 56 (Miss. 1916)).

234. *Id.* (citing *Thoenebe v. Mosby*, 101 A. 98 (Pa. 1917)).

to succeed where they can prove their injury to be “real, material, and substantial.”²³⁵

B. *Invasion of Privacy*

While privacy issues are beyond the scope of this Article, they are worth a mention. United States Senate Bill 631, the “Drone Aircraft Privacy and Transparency Act of 2017,” provides that “[t]he Secretary of Transportation shall establish procedures to ensure that the integration of unmanned aircraft systems into the national airspace system is done in compliance with the privacy principles.”²³⁶ While speaking at Oklahoma City University School of Law in September 2014, Supreme Court Justice Sonia Sotomayor called the changes in surveillance “frightening”:

There are drones flying over the air randomly that are recording everything that’s happening on what we consider our private property. That type of technology has to stimulate us to think about what is it that we cherish in privacy and how far we want to protect it and from whom.²³⁷

It may be true that a spying drone is a little creepy, but we are incidentally seen by people every day. We often end up in the background of someone’s cell phone video, and certainly internet browsers are recording our every move.²³⁸ “Drones’ size, price, and noisiness also make them faulty surveillance devices. If people want to spy, they’d achieve better results installing a hidden camera in a tree or on a windowsill.”²³⁹

VI. FUTURE FOR DRONE OPERATORS

The recent emergence of blockchain technology provides a potential solution to the increasing use of drones at low altitudes over private property. No matter the reason for drone operation, landowners could be able to financially capitalize this use of their low-altitude, private airspace. AERO Token is an Ethereum-based blockchain technology that

235. *See id.* (citing *Elmer v. S.H. Bell Co.*, 127 F. Supp. 3d 812, 825 (N.D. Ohio 2015)).

236. Drone Aircraft Privacy and Transparency Act of 2017, S. 631, 115th Cong. § 337 (applying privacy principles to commercial and public use, but not to news gathering or hobbyists), <https://www.congress.gov/bill/115th-congress/senate-bill/631/text>.

237. Sterbenz, *supra* note 25.

238. *Your ISP Is Tracking Every Website You Visit: Here’s What We Know*, PRIVACYPOLICIES.COM, <https://www.privacypolicies.com/blog/isp-tracking-you/> (last updated Aug. 6, 2019).

239. *Id.*

offers a glimpse of how blockchain can transform the aerial highway in the future.²⁴⁰ The company behind the AERO technology provides a way for landowners, known as “hosts,” to grant aviation easements for authorized drone service providers over private property.²⁴¹ Participants would make their airspace available on the blockchain and then generate additional income via digital currency each time they grant access for drones to pass through their airspace.²⁴²

The AERO Foundation proposes the use of uniform Revocable Aviation Easements, which would allow for landowners to grant access to commercial drone service providers within the AERO Network.²⁴³ The AERO Network is the platform through which the hosts and drone service providers operate.²⁴⁴ The AERO Network validates the hosts’ requests to allow use of private airspace and then notifies all drone service providers of low-altitude airspace availability.²⁴⁵ Drone service providers may also request permission to enter specific navigable airspace if a host has not initially authorized use on the network.²⁴⁶ The additional income generated by this network benefits the government in addition to hosts and operators. Income from temporary easements is treated as rental income under IRS tax laws in the United States, which is generally taxed as regular income.²⁴⁷ Although it is not widely used and accepted at the moment, the AERO Token Network provides a framework that could benefit all parties involved. Landowners can be compensated for allowing use of their private airspace, drone operators would be given a clear flight pattern that would reduce the possibility of trespass, and the government could collect extra income taxes from easement income.

Missy Cummings, professor of mechanical engineering and director of the Humans and Autonomy Lab at Duke University suggests that “perhaps Starbucks could be your intermediary point. You’re not really going to deliver to everyone’s home. Do you want drones to land in a backyard with a dog?”²⁴⁸ Just as Amazon has Amazon lockers for its standard automobile deliveries,²⁴⁹ maybe those centers will need to be

240. HAYLEY HALPIN ET AL., AERO TOKEN, CREATING A DRONE SUPERHIGHWAY USING THE BLOCKCHAIN (2017), https://icosbull.com/whitepapers/3110/AERO_Token_whitepaper.pdf.

241. *Id.*

242. *Id.* at 12.

243. *Id.* at 21.

244. *Id.* at 30.

245. *Id.* at 32.

246. *Id.* at 30.

247. See I.R.S. Priv. Ltr. Rul. 201250008 (Dec. 14, 2012).

248. Knight, *supra* note 30.

249. John-Michael Bond, *Amazon Locker Ensures You Never Have Another Package Stolen*, DAILY DOT (Feb. 23, 2018, 5:45 AM), <https://www.dailydot.com/debug/what-is-amazon-locker/>.

attended by someone who could meet a drone, take the package, and send it back on its way.

CONCLUSION

When drones burst onto the scene, they blurred the lines in an already grey area of the law—the intersection of uncontrolled navigable airspace and property rights. The historical belief was that the property held by an owner on the ground extended all the way to the heavens, but that is no longer the case.²⁵⁰ Technology has developed at a blistering pace, first through architectural feats, then air travel, and now through drone usage. With each new technological development, the courts face difficult challenges in determining the precise rights of landowners.

Drones have made matters even more difficult because operators use them for such a wide variety of reasons. Many governmental bodies, such as police, fire departments, and search and rescue units, use them for public-safety concerns.²⁵¹ Many private companies are rapidly increasing their use of drones for operations, ranging from building or site inspections, land surveying, or package delivery.²⁵² Drones have also taken hobbyists by storm, who operate them to take pictures or simply for fun.²⁵³ One thing is for certain: Drones are here to stay.

The FAA has tried to provide some clarity for drone operators through their airspace classifications of controlled airspaces: Classes A through E, and the uncontrolled Class G airspace in which UAVs operate.²⁵⁴ In addition, current FAA legislation states that unless a waiver is obtained to operate BVLOS, UAV operators must keep their drones within VLOS.²⁵⁵ However, it is easy for drone operators to violate these restrictions with the advanced technology that drones possess.

The huge number of drones operating in the United States also presents a great challenge for the courts because there is so little legislation and minimal precedent regarding their use. Many analogous cases addressing aerial trespass that drone operators could use in courts of law were decided over fifty years ago—way before drones were even a thought.²⁵⁶ Moving forward, the number of cases dealing with aerial drone trespasses will likely greatly increase because of the explosion of UAV popularity and the lack of concrete enforcement measures.

250. *E.g.*, *Pyramid Coal Corp. v. Pratt*, 99 N.E.2d 427 (Ind. 1951).

251. *See* Franzen, *supra* note 43; *see also* Nelson, *supra* note 43.

252. *See* IDENTIFIED TECHS., *supra* note 47; Frumkin, *supra* note 50; Knight, *supra* note 30.

253. *See* Schloss, *supra* note 24.

254. FED. AVIATION ADMIN., *supra* note 77.

255. FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 336, 126 Stat. 11, 77 (2012).

256. *See supra* Section III.A.

AERO Network provides a potential model that could create a consensus among private landowners and drone operators, as both sides would benefit. Although currently promoted through blockchain technology that many citizens do not yet understand, the AERO Network could benefit every party that has a stake in UAV use. Through this network, private landowners gain AERO Tokens, a digital currency, for allowing use of their low-altitude, navigable airspace.²⁵⁷ Drone operators can have peace of mind operating their UAVs through airspace with the consent of landowners. Finally, the government will benefit by receiving extra income tax dollars through income earned from the temporary avigation easements.²⁵⁸ After all, real estate developers have been trading in airspace rights for years and have annexed airspace above and around development properties for fees that can be many millions of dollars.²⁵⁹

The possibilities that drones provide are exciting for the future. However, courts are just beginning to feel the ramifications of this new technology. They have little concrete guidance in their decisions regarding what constitutes privately owned airspace. Furthermore, enforcement is and will be extremely difficult if they follow previous analogous court rulings, which hold that a mere intrusion by as little as one foot is a trespass.²⁶⁰ Drones are not going away, so courts, state legislatures, and the federal government must come together to provide clarity to drone operators and private landowners concerning their rights.

257. HALPIN ET AL., *supra* note 240, at 28.

258. *See id.* at 12.

259. Finn, *supra* note 68 (“Air rights are, in actuality, not fluffy chunks of available or orphaned air. They are unused or excess development rights gauged, like building density or lot size, by the square foot and transferable, when zoning permits it, from one buildable lot to another.”).

260. *Ellis v. Loftus Iron Co.* [1874], 10 LRCP 10 (Eng.).

WE NEED TO TALK ABOUT DATA: HOW DIGITAL MONOPOLIES ARISE AND WHY THEY HAVE POWER AND INFLUENCE

Daniel McIntosh

Abstract

Over the last 10 years, while we have seen the emergence of digital technologies able to improve human welfare, we have also seen the unparalleled concentration of that technology into the hands of a few global behemoths such as Microsoft, Google, Amazon, Facebook, and Apple (Big Tech). However, we would be wise to tame this runaway concentration of power in Big Tech; the recent revelations about the role that Facebook data played in the United States presidential election provides a stark illustration as to why.

This Article will analyze how and why the monopolization of digital technology occurred. In particular, this Article examines the role of intangible property, such as data and intellectual property, as well as the phenomenon known as the “network effect.” Intellectual property has been suspected of driving the monopolization of digital platforms. However, intellectual property is normally an afterthought and does little to prevent competition with the core business of Big Tech companies. Rather, what allows these companies to monopolize their business is the network effect acting on data in a positive feedback loop.

Dealing with the problems of a network effected market has always been difficult. In the past, competition regulations were the go-to tools. However, such regulations have so far proven largely ineffective because data does not fit squarely into traditional economic models. The other traditional alternative was consumer law. Even though we will soon see the implementation of stricter data protection laws with the introduction of the GDPR in Europe, its primary focus is on individual privacy, not monopolized power.

This Article will argue that the reason for the ineffectiveness of laws to deal with some of the harmful effects of Big Tech monopolies is that there is something about monopolies on data that is inherently different from other more benign goods or services. Data is information. It is this distinctive characteristic of data that has implicated Big Tech monopolization across such a broad range of fields, including personal privacy, democracy, security, innovation stifling, hacking, political influence, and media. So, while re-imagined competition and consumer regulations may work to prevent inflated prices and Draconian privacy policies, they will not address the more pressing problems of Big Tech monopolies on data.

INTRODUCTION	186
I. THE DRIVERS OF MONOPOLIZATION.....	189
A. <i>Intellectual Property</i>	189
B. <i>The Network Effect</i>	191
C. <i>Data Driven Network Effect</i>	193
II. CURRENT MEASURES	195
A. <i>Introduction</i>	195
B. <i>Competition Law</i>	195
C. <i>Consumer Law</i>	198
D. <i>Inadequacy of Current Regulations</i>	200
III. WE NEED TO TALK ABOUT DATA	201
A. <i>Data Is Different</i>	201
B. <i>Data Is Big</i>	202
C. <i>Facebook Case Study</i>	204
D. <i>Google Case Study</i>	206
E. <i>Data as Something More</i>	208
IV. SOLUTIONS	209
A. <i>Changing Our View of Data</i>	209
B. <i>Time Limiting Data</i>	209
C. <i>Thinking of Data as a Commodity, Labor,</i> <i>or a Human Right</i>	210
D. <i>Blockchain Technology</i>	211
CONCLUSION.....	213

INTRODUCTION

The digital age is here and its benefits offer a tantalizing glimpse of its promise to democratize institutions and provide increased access to information, tools, and power for all.¹ At its loftiest, the digital age may even empower the most underprivileged. But will we witness a revolution that tears down established institutions, or will we witness the introduction of a new technology that, like others before it, is ultimately controlled by an elite few?

1. KAREN MOSSBERGER ET AL., DIGITAL CITIZENSHIP: THE INTERNET, SOCIETY, AND PARTICIPATION (2008); Dirk Helbing & Evangelos Pournaras, *Build Digital Democracy*, 527 NATURE 33 (2015).

Digital technology has provided universal and widespread empowerment in an extremely short amount of time, a phenomenon that has not occurred arguably since the invention of the printing press.² The Organisation for Economic Co-operation and Development (OECD) recently described digital technology as having “as much importance as electricity, water, [and] highways.”³ A 2012 World Bank report on international development said that “[m]obile communication has arguably had a bigger impact on humankind in a shorter period of time than any other invention in human history.”⁴ For example, a middle class African in Kenya has access to the same iPhone owned and used by tech billionaire Elon Musk.⁵

It would not be an overstatement to say that digital technology has the power to solve, or at least substantially ameliorate, the current challenges we face. Such challenges include the environment, gender inequality,⁶ institutionalized tyranny, disease, and inequitable civil participation.⁷ To ensure digital technology reaches its potential, we must push and pull the appropriate levers.

At the birth of digital technology in the nineties, there was great excitement about the internet and its ability to free people. It would be democratic and open. However, this rosy optimism was perhaps a little premature. Now, in 2019, we are in the midst of an era in which large technology companies penetrate and influence the citizenry in ways not previously possible for private enterprises.

The top five most valuable companies in the world are no longer real estate owners or oil companies, but the Big Tech companies: Apple,

2. In Africa, mobile telephone usage went from two percent in 2000 to around ninety percent in 2014. Murithi Mutiga & Zoe Flood, *Africa Calling: Mobile Phone Revolution to Transform Democracies*, GUARDIAN (Aug. 8, 2016, 2:00 PM), www.theguardian.com/world/2016/aug/08/africa-calling-mobile-phone-broadband-revolution-transform-democracies.

3. Org. for Econ. Co-Operation and Dev. [OECD], *Big Data: Bringing Competition Policy to the Digital Era: Note by Annabelle Gawer*, at 15, DAF/COMP/WD(2016)74 (Dec. 16, 2016) [hereinafter *Gawer Note*], [https://one.oecd.org/document/DAF/COMP/WD\(2016\)74/en/pdf](https://one.oecd.org/document/DAF/COMP/WD(2016)74/en/pdf).

4. WORLD BANK, INFORMATION AND COMMUNICATIONS FOR DEVELOPMENT 2012: MAXIMIZING MOBILE 11 (2012).

5. *Cell Phones in Africa: Communication Lifeline*, PEW RESEARCH CTR. (Apr. 15, 2015), www.pewglobal.org/2015/04/15/cell-phones-in-africa-communication-lifeline.

6. Those working in international development continually explain that the best way to end poverty is the education of women. Surely digital technology is the greatest tool for doing so in countries where cultural norms and dogma make it difficult. See, e.g., Ana Revenga & Sudhir Shetty, *Empowering Women Is Smart Economics*, FIN. & DEV., Mar. 2012, at 40.

7. MARTA POBLET & ENRIC PLAZA, DEMOCRACY MODELS AND CIVIC TECHNOLOGIES: TENSIONS, TRILEMMAS, AND TRADE-OFFS (2017), https://www.researchgate.net/publication/317164590_Democracy_Models_and_Civic_Technologies_Tensions_Trilemmas_and_Trade-offs.

Alphabet,⁸ Microsoft, Amazon, and Facebook.⁹ In just the first quarter of last year, these five companies amassed \$25 billion USD in profits.¹⁰ Only fifteen years ago, Facebook did not exist, Google had only a loyal following,¹¹ and Amazon was just selling a few books.

There is now a widespread feeling, both in the public and in the mainstream press, that Big Tech has too much power over many aspects of our lives.¹² The recent revelations about the role that Facebook data played in the United States presidential election provides one disturbing example of the platforms.¹³ Google has been able to monopolize information in other ways, placing itself in prime position to capitalize on future innovation, especially in the field of artificial intelligence (AI).¹⁴ Most of the concerned discussion has centered around the various manifestations of data monopolization, such as data privacy, media influence, and lack of consumer choices. However, few have been able to tease out precisely what it is that provides Big Tech with its power and influence.

This Article will analyze how and why the monopolization of digital technology has occurred. Part I examines the possible driving factors in the monopolization of digital technologies, focusing in particular on the contribution of intangible property, such as data and intellectual property, and the phenomenon known as the network effect. It is the network effect

8. Alphabet Inc. is Google's parent company.

9. As of March 2017, the market capitalization in USD are: (1) Apple: \$754 billion; (2) Google: \$579 billion; (3) Microsoft: \$509 billion; (4) Amazon: \$423 billion; and (5) Facebook: \$411 billion. PWC, GLOBAL TOP 100 COMPANIES BY MARKET CAPITALIZATION 32 (2017), <https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf>. See also, *The World's Largest Public Companies*, FORBES, www.forbes.com/global-2000/list/#header:marketValue_sortreverse:true (last visited Aug. 16, 2019).

10. *The World's Most Valuable Resource Is No Longer Oil, But Data*, ECONOMIST, May 6, 2017, at 9, <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

11. Lucy Hooker, *How Did Google Become the World's Most Valuable Company?*, BBC NEWS (Feb. 1, 2016), <https://www.bbc.com/news/business-35460398>.

12. See, e.g., Xavier Rizos, *The Age of Internet Empires*, ABC NEWS (Dec. 19, 2013, 5:21 PM), <https://www.abc.net.au/news/2013-12-20/rizos-the-age-of-internet-empires/5168818> (“[T]he internet has shifted from the free innovative market people still imagine towards a juxtaposition of private empires”); Robert B. Reich, Opinion, *Big Tech Has Become Way Too Powerful*, N.Y. TIMES (Sept. 18, 2015), <https://www.nytimes.com/2015/09/20/opinion/is-big-tech-too-powerful-ask-google.html>.

13. See David Folkenflik, *Facebook Scrutinized Over Its Role in 2016's Presidential Election*, NPR (Sept. 26, 2017, 4:59 AM), <https://www.npr.org/2017/09/26/553661942/facebook-scrutinized-over-its-role-in-2016s-presidential-election>.

14. Robert Wright, *Google Must Be Stopped Before It Becomes an AI Monopoly*, WIRED (Feb. 23, 2018, 8:00 AM), <https://www.wired.com/story/google-artificial-intelligence-monopoly/>.

that has provided Big Tech companies with their monopolies by acting on data in such a way as to create a data-opoly.

Part II discusses the current legal measures being utilized to combat such monopolization. While the two primary streams of law—consumer and competition law—are showing some positive progress in addressing problems associated with data monopolization, especially in the European Union (EU), they continue to focus on the symptoms rather than the causes of monopolization. This Article argues that the difficulty in dealing with data monopolies is likely due to the nature of data itself. As explained in Part III, it is the subject matter of the monopoly—big data, with its myriad of applications—that is the core of the power and influence of companies such as Google, Facebook, and Amazon. Part IV presents some solutions, the most promising being the use of digital technology itself, namely blockchain technology, to solve the problem of the monopolization of big data.

I. THE DRIVERS OF MONOPOLIZATION

A. *Intellectual Property*

Any analysis of the monopoly power of companies that work largely with intangible products¹⁵ requires an investigation of intellectual property—the legal demarcator of ownership of intangibles.¹⁶ Intellectual property is undoubtedly an imperative for tech companies, evidenced by the number and value of patents they own.¹⁷ However, of the monopolies

15. Google is not a product you can buy and put into your hands, Facebook is not a plumber fixing your toilet, and Amazon is not a shop whose shelves you can peruse. Tangible property, such as a bicycle or real estate, is physically exclusive. The owner (or user) of a bike will use it to the exclusion of all others as it cannot be used by others at the same time. Intangible property never finds itself in such a conundrum. This crucial difference is the reasoning behind the legal protection for intellectual property.

16. James Eyers, *Facing Up to the IP Tsunami*, AUSTL. FIN. REV., Aug. 11, 2009, at 61, https://www.wipo.int/export/sites/www/about-wipo/en/dgo/interviews/pdf/gurry_afr_09.pdf (explaining that intellectual property is set to become the basis of competition in the future); see also Manoj P. Dandekar, Managing Director, Enter. Econ. Evaluation, Presentation at the Society of Depreciation Professionals Annual Conference: Valuation of Intangible Assets and Intellectual Property (Sept. 11, 2017), https://c.yimcdn.com/sites/www.depr.org/resource/resmgr/2017_Conference/2017Presentations/MDandekarValuationIntangible.pdf (explaining that the definition of the intellectual property sets its boundaries and limits, that the boundaries represent the scope of the commercial intangible assets, and that—generally—the value and power of some companies should be evaluated based on the value of these intangible assets).

17. The key role intellectual property plays in digital technology can be evidenced by the number and value of patents owned by companies in digital technology. In the mid-1990s, the United States courts opened the door to allow software patents. By the end of the '90s, there were 20,000 software patents per year being granted in the United States. By 2013, that figure had tripled to 68,000 software patents. See James E. Bessen, *A Generation of Software Patents*, 18

that have presented themselves on the digital landscape, few trace their initial establishment to intellectual property. It is only after a company's rise to dominance and wealth that it seeks to bolster its position with intellectual property rights. For example, Microsoft had only five patents in its first fifteen years, while now—as a billion-dollar company—it applies for 2,000 patents annually.¹⁸ Similarly, Google's surprising \$12.5 billion purchase of Motorola—a stagnant company at the time—was largely considered to be motivated by the latter's 17,000 patents.¹⁹

Although these extensive intellectual property portfolios may inhibit competition,²⁰ they tend not to cover the core of a Big Tech monopoly's business. Take Facebook as an example. While it was arguably innovative in its initial concept in 2004,²¹ the core of Facebook's business today is scarcely protected by intellectual property apart from the trademark on its name. Facebook's website is not covered by any significant patents and its functionality could be re-coded over the course of a weekend by a group of Finnish teenagers.²² Even the appearance of

B.U. J. SCI. & TECH. L. 241, 253 (2012). Their wealth is also largely intangible. While more traditional large companies like McDonald's and Exxon may have had incredible wealth in land or machinery, the Big Tech companies are asset poor by comparison, clearly preferring intangible property. For example, in 2016, Apple had \$20 billion in cash, \$216 billion invested, and only \$27 billion in property, plants, and equipment. *Apple Company Financials*, NASDAQ, www.nasdaq.com/symbol/aapl/financials?query=balance-sheet (last visited Feb. 20, 2019). Indeed, Apple does not even care to own its factories. See Malcolm Moore, *Why Apple Can't Control Its Chinese Factories*, TELEGRAPH (Mar. 5, 2010, 7:27 AM), <https://www.telegraph.co.uk/technology/apple/7375684/Why-Apple-cant-control-its-Chinese-factories.html>.

18. Issie Lapowsky, *EFF: If You Want to Fix Software Patents, Eliminate Software Patents*, WIRED (Feb. 25, 2015, 9:00 PM), <https://www.wired.com/2015/02/eff-eliminate-software-patents/>.

19. Amir Efrati & Spencer E. Ante, *Google's \$12.5 Billion Gamble*, WALL ST. J. (Aug. 16, 2011), <https://www.wsj.com/articles/SB10001424053111903392904576509953821437960>; see also Brian Womack & Zachary Tracer, *Google Agrees to Acquire Motorola Mobility for \$12.5 Billion*, BLOOMBERG (Aug. 15, 2011, 4:48 PM), <https://www.bloomberg.com/news/articles/2011-08-15/google-agrees-to-acquisition-of-motorola-mobility-for-about-12-5-billion>.

20. Many commentators have pointed out that intellectual property is not particularly well-suited to encouraging innovation in the field of digital technology because unlike other fields such as pharmaceuticals, where the process of innovation is “long, risky and expensive,” it seems all you need to start a software company is a computer and, of course, a garage. See Steve Brachmann, *How Tech's Ruling Class Stifles Innovation with Efficient Infringement*, IPWATCHDOG (Mar. 17, 2017), <https://www.ipwatchdog.com/2017/03/17/tech-ruling-class-stifles-innovation-efficient-infringement/id=79391/>.

21. Sarah Phillips, *A Brief History*, GUARDIAN (July 25, 2007, 5:29 AM), <https://www.theguardian.com/technology/2007/jul/25/media.newmedia>.

22. Ravi Kumar, *How to Create Your Own Website like Facebook for Free?*, GET EVERYTHING, www.geteverything.org/how-to-create-your-own-website-like-facebook-for-free/ (last updated Oct. 20, 2017).

the website could, within limits, be copied without breaching the company's intellectual property.²³

Google finds itself in a similar situation. Google's initial PageRank²⁴ technology—developed by Larry Page and Sergey Brin as part of a Ph.D. project at Stanford University—was groundbreaking at the time and was rightly granted a patent.²⁵ Despite the impending expiration of the PageRank patent and the existence of superior search algorithms that competitors have already invented, however, nobody is questioning whether Google's search engine, which accounts for 85% of Google's \$136.2 billion USD revenue through advertising,²⁶ is under imminent competitive threat. The same lack of intellectual property protection applies to other dominant platforms such as Airbnb, Uber, eBay, and Amazon.

B. *The Network Effect*

If digital technology companies generating billions of dollars—whose functionalities can be so easily copied—are not protected at their core by intellectual property, what then is thwarting competitors? The broadly accepted answer is what economists call the network effect.²⁷

A network effect occurs where the benefit to a user of a product or service increases as the number of users increases, a sort of user begets user scenario.²⁸ A classic example is the fax machine. While the benefit of owning the first fax machines was minimal, the benefit increased

23. Mark Davison & Ian Horak, *Shanahan's Australian Law of Trade Marks and Passing Off* (5th ed. 2012).

24. Danny Sullivan, *What Is Google PageRank? A Guide for Searchers and Webmasters*, SEARCH ENGINE LAND (Apr. 20, 2007, 1:18 AM), <https://searchengineland.com/what-is-google-pagerank-a-guide-for-searchers-webmasters-11068>.

25. John Battelle, *The Birth of Google*, WIRED (Aug. 1, 2005, 12:00 PM), http://www.wired.com/wired/archive/13.08/battelle.html?pg=2&topic=battelle&topic_set=.

26. ALPHABET INC., ANNUAL REPORT (FORM 10-K) 7, 26–27 (2018), https://abc.xyz/investor/static/pdf/2017_google_annual_report.pdf?cache=5504fde.

27. Mark A. Lemley & David McGowan, *Legal Implications of Network Economic Effects*, 86 CAL. L. REV. 479, 481 (1998) (“A Network effect exists where purchasers find a good more valuable as additional purchasers buy the same good.”).

28. A network effected market is not always undesirable. There can be benefits from the enabling of interactions between a consumer and others who own the product. The “benefits of a purchaser, in other words, is access to other purchasers.” *Id.* at 488. For example, the Apple app ecosystem is a strongly network-effected market, yet there have been countless new and useful apps created by all levels of entrepreneurs and newcomers. See Daniel D. Garcia-Swartz & Florencia Garcia-Vicente, *Network Effects on the iPhone Platform: An Empirical Examination*, 39 TELECOMMS. POL'Y 877, 877–79 (2015) (discussing how Apple's business platform has grown under network effects).

exponentially as more people adopted the technology. Other examples include rail gauges and telephone lines.

Digital platforms have a high propensity to undergo network effects because they function on interoperability and communication with other similar products and users.²⁹ In the beginning, a new platform, a website service or app, needs to adequately meet some need. Then, the pervasiveness of the platform's use, which is the result of its initial success,³⁰ also serves as the driver for its further uptake.³¹ In the case of Microsoft Office, once it became the dominant word processor, user familiarity and software compatibility meant that more and more users were encouraged to adopt the product, resulting in an arguably inferior product at an inflated price.

While a network effect does not inevitably result in a "winner takes all" outcome,³² the consensus in the literature appears to be that for digital platforms like software and websites, the network effect is the main

29. A great example can be seen in keyboards. While the Dvorak keyboard has been shown to allow for a more rapid typing speed, the QWERTY keyboard is more widespread, making it not worthwhile for a typist to learn Dvorak typing. See Matthew T. Clements, *Inefficient Standard Adoption: Inertia and Momentum Revisited*, 43 ECON. INQUIRY 507, 507–08 (2005), <https://onlinelibrary.wiley.com/doi/epdf/10.1093/ei/cbi034>.

30. See Lemley & McGowan, *supra* note 27, at 495–96; see Paul Klemperer, *Network Effects and Switching Costs: Two Short Essays for the New Palgrave* (Mar. 2005) (unpublished essays), www.nuffield.ox.ac.uk/users/klemperer/NewPalgrave.pdf.

31. Economic modeling has shown that, in this way, a market share of 40% can lead to an almost automatic increase to 80% of the market share. Timing is important, as the first-mover or best-timed product—rather than the superior product—is often triumphant. See John T. Soma & Kevin B. Davis, *Network Effects in Technology Markets: Applying the Lessons of Intel and Microsoft to Future Clashes Between Antitrust and Intellectual Property*, 8 J. INTEL. PROP. L. 1, 3, 46 (2000).

32. See Gawer Note, *supra* note 3, at 9. In the OECD Committee Hearing, Germany noted that the network effect may lead to a winner takes all scenario, while Professor Annabelle Gawer explained that this is also not a given and there are many "counterexamples of markets with network effects that have not been monopolised." Org. for Econ. Co-Operation and Dev. [OECD], *Summary of Discussion of Hearing on Big Data: Annex to the Summary Record of the 126th Meeting Competition Committee*, at 2, 5, DAF/COMP/M(2016)2/ANN2/FINAL (Apr. 26, 2017) [hereinafter *OECD Big Data Hearing Summary*], [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/M\(2016\)2/ANN2&docLanguage=En2](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DAF/COMP/M(2016)2/ANN2&docLanguage=En2) (2017). Further, the OECD reports that "the very specific features of the digital economy imply that, in many cases, firms compete for the market instead of competing in the market, leading to 'winner takes all' outcomes, as it was observed when Facebook was able to displace Myspace as the most popular social network. Org. for Econ. Co-Operation and Dev. [OECD], *Big Data: Bringing Competition Policy to the Digital Era: Background Note by the Secretariat*, at 17, DAF/COMP(2016)14 (Oct. 27, 2016) [hereinafter *Background Note by the Secretariat*].

determinate of market dominance.³³ As tech billionaire and Facebook's first outside investor Peter Thiel says, "competition is for losers."³⁴ His recommendation: "If you want to create and capture lasting value, look to build a monopoly."³⁵

C. Data Driven Network Effect

The network effect needs a network. The network effects observed previously were due to physical manifestations such as telephone lines or rail gauges.³⁶ More recently, a new form of network effect has loomed into view in the digital world. It is conceptually similar to the walled gardens of intellectual property seen in early digital technology: a network effect not in relation to compatibility, but rather, in relation to data. The data-opoly.³⁷

Markets with a high reliance on data are experiencing positive feedback loops: the more data an enterprise has, the better the product. This leads to strong data-driven network effects. A search engine like Google is able to improve its search results by using the immense data its search database continually collects from its billions of users.³⁸ This may include popular search queries that are easily answered, as well as the more obscure and rare searches that can only be well served with gigantic datasets. The same principle enables Facebook to improve its content and to target users with sublimely specific advertising on account of the sheer volume of user data it possesses.³⁹

With so many inputs, big data and its processing are now capable of what is known as "now-casting":⁴⁰ real-time forecasting of traffic conditions, restaurant crowds,⁴¹ or flu outbreaks. Discovering such information requires a huge volume of data from which the data of

33. Maurice E. Stucke & Allen P. Grunes, *Data-opolies* 8, 11 (Univ. of Tenn. Legal Studies Research, Paper No. 316, 2017), <https://ssrn.com/abstract=2927018>.

34. Peter Thiel, *Competition Is for Losers*, WALL ST. J. (Sept. 12, 2014, 11:25 AM), www.wsj.com/articles/peter-thiel-competition-is-for-losers-1410535536.

35. *Id.*

36. Note, *Smith v. Illinois Bell Telephone Company: A Development in the Law of Public Utilities*, 44 HARV. L. REV. 833, 834 ("Of utilities, the telephone industry presents the most notable instance of centralized organization and monopolistic control.").

37. See MAURICE E. STUCKE & ALLEN P. GRUNES, *BIG DATA AND COMPETITION POLICY* (2016) (coining the term "data-opoly"); see also Stucke & Grunes, *supra* note 33.

38. Stucke & Grunes, *supra* note 33, at 6.

39. See *id.* at 11.

40. Now-casting is defined as "the prediction of the present, the very near future and the very recent past." Marta Banbura et al., *Now-Casting and the Real-Time Data Flow*, in 2 HANDBOOK OF ECONOMIC FORECASTING 195, 196 (Graham Elliott & Allan Timmermann eds., 2013).

41. See sources cited *supra* note 32.

interest can be extracted. Otherwise, the data would be collected at too low a frequency to enable now-casting.

Size matters when it comes to data. Stucke and Grunes demonstrate that a poorly designed algorithm can find more valuable information and insights in high volumes of various data than a superior algorithm can when working with a cleaner, but smaller, dataset.⁴² Google's chief scientist admitted: "We don't have better algorithms than anyone else. We just have more data."⁴³ The end result is that consumers may be locked into using a dominant service such as Google rather than their preferred service, which may offer them better privacy options or less advertising.

This is why Facebook, Google, and Amazon offer their social, search, and e-commerce platforms for free. Rather, they receive user data as their remuneration. So, although Google,⁴⁴ Microsoft,⁴⁵ and Facebook⁴⁶ often claim that competitors can easily gather their own data and that competition is therefore just "one click away"⁴⁷ because "data is not valuable *per se*,"⁴⁸ the evidence increasingly suggests otherwise.⁴⁹ If data were not valuable, there is little to explain why Facebook paid \$16 billion USD to purchase WhatsApp, a company of only 60 employees and no assets.⁵⁰ In reality, data is acting as an entry barrier to many

42. STUCKE & GRUNES, *supra* note 37, at 23.

43. Matt Asay, *Tim O'Reilly: "Whole Web" Is the OS of the Future*, CNET (Mar. 18, 2010), www.cnet.com/news/tim-oreilly-whole-web-is-the-os-of-the-future/ (quoting Peter Norvig, chief scientist at Google).

44. OECD *Big Data Hearing Summary*, *supra* note 32, at 3 ("[D]ata does not necessarily act as a barrier to entry since, regardless of its size, data is nowadays very cheap to collect, can be easily generated . . .") (statement of Hal Varian, Chief Economist at Google and Professor at Berkeley School of Information).

45. *Id.* at 4 ("[D]ata is abundant and has only value when properly structured and categorised.") (statement of Chris Meyers, Associate General Counsel of Antitrust from Microsoft).

46. *See* Case M.7217, Facebook/WhatsApp, 2014 EUR-Lex CELEX LEXIS 32104M7217, 12 (Mar. 10, 2014).

47. Eric Schmidt, *Why Google Works*, HUFFINGTON POST (Jan. 20, 2015, 4:14 PM), www.huffingtonpost.com/eric-schmidt/why-googleworks_b_6502132.html.

48. OECD *Big Data Hearing Summary*, *supra* note 32, at 3 (statement of Prof. Hal Varian).

49. *Id.* at 2 ("Big Data has blurred the line between [supply and demand] allowing users of an online service to behave simultaneously as consumers and suppliers of data. In turn, that data can be immediately used by the service provider to improve the quality of the service, leading to a real-time feedback loop that was not observed before.")

50. *Facebook to Acquire WhatsApp*, FACEBOOK (Feb. 19, 2014), <https://newsroom.fb.com/news/2014/02/facebook-to-acquire-whatsapp/>.

competitors.⁵¹ In 2016, the OECD, the French Autorité de la Concurrence, and the German Bundeskartellamt all acknowledged the existence of data-driven networks and that they give a competitive advantage over rivals.⁵²

II. CURRENT MEASURES

A. Introduction

The law is struggling to find solutions to the new challenges of Big Data.⁵³ In the context of privacy and security of big data, as explained by one commentator, current legislation “is still grounded in, and focused upon the twentieth century’s responses—to the . . . processing and distribution of data . . .”⁵⁴

The current legislative go-to tools of regulators to combat data monopolization are competition law and consumer law. As discussed below, competition law is arguably ineffective at resolving intellectual property and network-effected monopolies, and seems even less equipped to deal with data because it currently has no real market. With the soon to be introduced EU General Data Protection Regulation (GDPR),⁵⁵ consumer law is shaping up to be a sharper tool for willing regulators. But at its heart, it remains a bastion of the individual consumer versus Big Tech and does not consider the impact of Big Data monopolization from the perspective of the bigger picture of creating a better society.

B. Competition Law

Prior to the arrival of data-opolies, there had been some partial success in limiting network effects using competition regulations, or antitrust laws as it is known in the United States. In the late nineties, Microsoft held an 80% market share.⁵⁶ However, on the back of an antitrust suit, the

51. Stucke & Grunes, *supra* note 33, at 2–6; Inge Graef, *Market Definition and Market Power in Data: The Case of Online Platforms*, 38 *WORLD COMPETITION* 473, 473 (2015).

52. Autorité de la Concurrence & Bundeskartellamt, *Competition Law and Data*, at 15–16 (May 10, 2016), https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2.

53. *See generally id.*

54. Pompeu Casanovas et al., *Regulation of Big Data: Perspectives on Strategy, Policy, Law and Privacy*, 7 *HEALTH & TECH.* 335, 340 (2017).

55. *See* 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) 1.

56. Tim Worstall, *Microsoft’s Market Share Drops from 97% to 20% in Just over a Decade*, *FORBES* (Dec. 13, 2012, 11:16 AM), <https://www.forbes.com/sites/timworstall/2012/12/13/>

United States government was able to persuade Microsoft to share its programming interfaces with other companies.⁵⁷

There is a glut of analysis on the effectiveness of competition regulations as applied to digital technologies prior to the emergence of Big Data.⁵⁸ The inadequacies of these regulations in addressing network-effected markets, however, has been attributed to the features unique to a network-effected monopoly that differ from a natural monopoly.⁵⁹ In the case of a natural monopoly, as demand increases, the margins decrease according to classic economic principles of the scale of production, whereas in a network-effected market, value is added by existing users through increased demand.⁶⁰

The literature reveals that while the lawmakers recognized the outcome—the monopoly—they struggled⁶¹ with understanding the contribution of the network effect. Even by 2001, “[o]nly a few courts in antitrust cases [had] recognized the existence of network effects, and attempted to factor it into their analysis.”⁶² Further, the Federal Trade Commission (FTC) has not lodged a serious case against Big Tech this century. Consequently, they largely failed in limiting the prevalence of network-effected markets. Perhaps the most compelling evidence is the fact that the five most valuable companies in the world today are Big Tech companies⁶³ who owe a large part of their value to network effects.

Even apart from dealing with the complexities of a network market, there is the additional difficulty that data, unlike word processing software, is currently not valued. When most of the services in question

microsofts-market-share-drops-from-97-to-20-in-just-over-a-decade/#6409340351cf.

57. See *United States v. Microsoft Corp.*, 980 F. Supp. 537, 539–40 (D.D.C. 1997).

58. E.g., Ariel Katz, Making Sense of Nonsense: Intellectual Property, Antitrust, and Market Power, 49 ARIZ. L. REV. 837 (2007); Emanuela Arezzo, Intellectual Property Rights at the Crossroad Between Monopolization and Abuse of Dominant Position: American and European Approaches Compared, 24 J. MARSHALL J. COMPUTER & INFO. L. 455 (2006); Lemley & McGowan, *supra* note 27.

59. Lemley & McGowan, *supra* note 27, at 484 (“While the two problems may be difficult to distinguish in practice—and some courts may treat them the same—the two cases are analytically distinct and therefore may require different legal treatment . . .”).

60. *Gawer Note*, *supra* note 3, at 9; Soma & Davis, *supra* note 31, at 5.

61. Lemley & McGowan, *supra* note 27, at 485 (“The theoretical implications of network markets have not been fully elaborated even in the economic literature. The theoretical legal analysis that has drawn upon such literature is even less complete, and empirical data on the behavior of firms and consumers in network markets is scarcer still.”).

62. Soma & Davis, *supra* note 31, at 6.

63. Lucinda Shen, *Here Are the Fortune 500’s 10 Most Valuable Companies*, FORTUNE (May 21, 2018), <http://fortune.com/2018/05/21/fortune-500-most-valuable-companies-2018/>.

are offered for free to its users and the data collected is not later sold, it is “particularly difficult”⁶⁴ to assess market power and value.⁶⁵

However, there has been a notable change in Europe in the last two years. There is now a growing recognition that data can be used as a barrier to entry and that data-opolies are problematic.⁶⁶ Last year, the European Commission handed Google a record-breaking €2.42 billion fine for abusing its dominance as a search engine by giving illegal competitive advantage to its own services in the lucrative online shopping market.⁶⁷

In November 2016, addressing concerns raised by Big Data and data-driven network effects, the OECD conducted an investigation into what it considered a “first step in a broader work stream”⁶⁸ in “identifying some of the competition challenges from the increasing use of consumer data for business purposes, and to discuss possible reactions by competition authorities and other agencies.”⁶⁹ The report outlines its view that the problem of too much concentration of data in so few companies could be best remedied with appropriately adapted competition laws.⁷⁰ The report states that “[t]raditional antitrust tools can be adapted and applied to tackle such data-related anticompetitive practices, by treating data as any other input. For instance, in merger control and exclusionary abuse cases, competition authorities may consider the risks of foreclosure and design remedies accordingly.”⁷¹

64. *Background Note by the Secretariat, supra* note 32, at 16.

65. In collecting the data itself, the platform is not doing anything that is considered anti-competitive under the traditional analysis. This is precisely why the EU regulator decided to look no further when assessing any possible anti-competitive issues regarding the aforementioned \$19 billion USD Facebook/WhatsApp merger. Facebook answered all concerns by showing they did not sell data or charge for their services. *See* Case M.7217, *supra* note 46, at 12.

66. *See, e.g.,* Stucke & Grunes, *supra* note 33, at 5–6; Autorité de la Concurrence and Bundeskartellamt, *supra* note 52, at 11.

67. European Commission Press Release IP/17/1784, Antitrust: Commission Fines Google €2.42 Billion for Abusing Dominance as Search Engine by Giving Illegal Advantage to Own Comparison Shopping Service (June 17, 2017), europa.eu/rapid/press-release_IP-17-1784_en.htm.

68. *Background Note by the Secretariat, supra* note 32, at 5.

69. Org. for Econ. Co-Operation and Dev. [OECD], *Big Data: Bringing Competition Policy to the Digital Era: Executive Summary*, at 4, DAF/COMP/M(2016)2/ANN4/FINAL (Apr. 26, 2017) [hereinafter *OECD Executive Summary*], [https://one.oecd.org/document/DAF/COMP/M\(2016\)2/ANN4/FINAL/en/pdf](https://one.oecd.org/document/DAF/COMP/M(2016)2/ANN4/FINAL/en/pdf).

70. *Background Note by the Secretariat, supra* note 32, at 5 (noting that initially, the concerns of big data and its implications were around consumer protection, but that after several high-profile mergers and the increasing amount of monopolization and control of data, the outcome on competition and the broader implications for markets need to be considered.).

71. *OECD Executive Summary, supra* note 69, at 4.

In the same way, Graef suggests a reworking of competition law to where, instead of looking at purely price indications of monopoly, it would look at other qualities in determining when antitrust provisions should be triggered.⁷² More recently, in December 2017, Germany's Federal Cartel Office, the Bundeskartellamt, made its preliminary assessment that Facebook was using its dominance to extort personal data from users by bullying them into agreeing to their unfavorable privacy terms and conditions.⁷³ This is likely to be the first time a regulator is using data as a measure of anti-competitive practices.

C. Consumer Law

Consumer law protections are also routinely cited in data regulation discourse. Amongst the literature, there is an acknowledgement that collection of data and its misuse may harm consumer interests, including privacy, data protection, freedom of speech, consumer choice, and non-discrimination rights.⁷⁴ The OECD summarizes the situation as follows:

The development of the digital economy and of Big Data has raised concerns that users of online services may lose control over the way that their data is collected and used. In the absence of a regulatory framework that promotes transparency and consumer's control over their own data, there is a risk of undermining the good functioning of the digital markets.⁷⁵

The introduction of the GDPR on May 25, 2018, initiated deep and sweeping changes into how personal data is managed in Europe and for

72. Graef suggests a more objective measure of the data power of an enterprise would be to "look at their ability to monetize the collected information. The revenue gained by a provider through licensing of data to third parties, delivering targeted advertising services or offering other paid products and services to customers having data as input indicates how successful it is in the market." Graef, *supra* note 51, at 502.

73. The case had not been finalized at the time of the preliminary assessment. The Bundeskartellamt gave Facebook time to respond and negotiate. The proceedings were administrative, not offense proceedings with the potential for fines. Bundeskartellamt Press Release, *Preliminary Assessment in Facebook Proceeding: Facebook's Collection and Use of Data from Third-Party Sources Is Abusive* (Dec. 19, 2017), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2017/19_12_2017_Facebook.html.

74. Executive Summary of the Opinion of the European Data Protection Supervisor on Effective Enforcement in Digital Society Economy, 2016 O.J. (C 463) 8, 8, [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XX1213\(01\)&qid=1565004591543&from=EN](https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016XX1213(01)&qid=1565004591543&from=EN); *European Data Protection Supervisor Opinion on Coherent Enforcement of Fundamental Rights in the Age of Big Data*, at 5 (Sept. 23, 2016), https://edps.europa.eu/sites/edp/files/publication/16-09-23_bigdata_opinion_en.pdf.

75. OECD *Executive Summary*, *supra* note 69, at 5.

EU citizens.⁷⁶ The aim of the GDPR is to give EU citizens far-reaching rights and control over their personal data.⁷⁷ The strict data compliance framework will be enforced by severe penalties of up to €20,000,000, or in the case of an undertaking, up to four percent of the total worldwide annual turnover,⁷⁸ which could potentially mean millions or even billions of euros in fines. These strong sanctions perpetuate the EU's increased willingness to regulate Big Tech—something yet to be seen in the U.S.

The GDPR provides citizens various rights in relation to their data, namely, the right of access to their personal data,⁷⁹ the right to be forgotten,⁸⁰ a requirement that consent to collect personal data be freely given,⁸¹ a right to notification of any data breach,⁸² and a right not to be subject to a decision based solely on automated processing.⁸³ Most significantly, the GDPR introduces a “data portability right,” which gives a person the right to be able to transfer his or her personal data from one provider to another.⁸⁴ This data portability was introduced with individual rights in mind. However, it may have a significant impact on competition as users are able to easily switch platforms. Thus, the GDPR operates in the “intersection between data protection and other fields of law (competition law, intellectual property, consumer protection, etc).”⁸⁵

Personal data portability is novel—it has no precedent in any previous framework of law.⁸⁶ The GDPR gives no mechanism for effectuating portability other than that data must be in a “commonly used and machine-readable format and . . . [transmitted] to another controller without hindrance”⁸⁷ It remains to be seen how data controllers will execute the portability.

76. Dale Walker & Keumars Afifi-Sabet, *What Is GDPR? Everything You Need to Know, from Requirements to Fines*, ITPRO (July 23, 2019), <https://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know>.

77. *Id.*

78. Regulation 2016/679, *supra* note 55, at 83.

79. *Id.* at 43.

80. *Id.* at 43–44 (“The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay . . .”).

81. *See id.* at 37.

82. *Id.* at 52–53.

83. *Id.* at 46.

84. *Id.* at 45; Paul De Hert et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 *COMPUTER L. & SECURITY REV.* 193, 194 (2018).

85. De Hert et al., *supra* note 84, at 193.

86. *See id.* at 203.

87. Regulation 2016/679, *supra* note 55, at 45.

De Hert argues that the right to data portability may have two possible scenarios.⁸⁸ The first would require only the transfer of “provided” personal data. In contrast, the second and wider scenario would require the transfer of all data, including data that is generated from the personal data.⁸⁹ In supporting the latter, broader definition, De Hert says:

This scenario does not only encourage a real competition between service providers (limiting barriers for users willing to change service in the digital market), but it also avoids the monopolisation of the Internet by large companies, by encouraging interoperable formats, developing multilevel platforms where the centre is the user and the actors are different service providers.⁹⁰

However, as the implementation of the GDPR is considered to be its biggest challenge and greatest unknown,⁹¹ it is difficult to predict any impact it will have on reducing data monopolization. Furthermore, the real aim of the GDPR is to protect personal privacy—not to regulate competition by proxy. Finally, only personal data falls within its gambit⁹² and so it will not address problems on monopolization of big data generally.

D. *Inadequacy of Current Regulations*

This two-pronged regulatory approach, using appropriately retooled antitrust and consumer laws, shows promise in reducing the monopolistic state of digital platforms, particularly in Europe where regulators are starting to show some real teeth. In practice, however, both streams of law are ill-equipped to fully resolve the issues of big data monopolization because they merely address the downstream manifestations of big data, but not the origin of the problem: the monopoly itself. Consumer law may ensure users have better privacy policies and competition law may prevent large anticompetitive mergers, though this remains to be seen. Perhaps even a version of media pluralism laws could ensure that large platforms do not have so much media influence. However, even if successful, the other downstream consequences of big data monopolization will remain.

88. De Hert et al., *supra* note 84, at 202.

89. *Id.*

90. *Id.*

91. *See id.* at 194.

92. *See* Miranda Mourby et. al., *Are “Pseudonymised” Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK*, 34 *COMPUTER L. & SECURITY REV.* 222, 222 (2018) (discussing whether Article 4(5) of the GDPR, dealing with “pseudonymization,” will have the effect of expanding the scope of personal data).

Most notably, Big Data is set to become key for future innovation and growth.⁹³ Especially in the field of artificial intelligence, companies such as Google have an enormous head start, as Big Data is the fuel from which artificial intelligence runs.⁹⁴ For example, Tesla collects data from its cars which it then uses to optimize its self-driving algorithms and thus operates in a data-driven, network-effected market—making it difficult for competitors to innovate ahead of Tesla.⁹⁵ However, this application of big data does not appear on the radar of antitrust or consumer law.

This is why Stucke questions “whether competition law is the appropriate tool for dealing with issues arising from the use of Big Data.”⁹⁶ Part of the failure of competition law is likely to be that Big Data is just so new—its usefulness and implications are only a few years old. It is only in the last two years that legal scholars and governments have begun to discuss the issue of monopoly ownership of Big Data as a problem in itself.⁹⁷ Thus, while the OECD investigation of data monopolies pondered how to ensure that monopolies face “competitive pressure to constantly improve their products and preserve low prices,”⁹⁸ it made no mention of the distinction in power and influence between Facebook and Uber.

III. WE NEED TO TALK ABOUT DATA

A. *Data Is Different*

Efforts thus far to address the consequences of the centralized power of Big Tech have attended to the symptoms, but not the underlying problem. Data monopolies are different from previous monopolies because there is another dimension to the nature of data that other, more benign goods or services do not have. It is the nature of the data itself—

93. JAMES MANYIKA ET AL., MCKINSEY GLOB. INST., *BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY* 2, 6 (2011), https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx (“[O]ur research suggests that we are on the cusp of a tremendous wave of innovation, productivity, and growth The use of big data is becoming a key way for leading companies to outperform their peers. For example, we estimate that a retailer embracing big data has the potential to increase its operating margin by more than 60 percent.”).

94. Christian Ehl, *Data—the Fuel for Artificial Intelligence*, MEDIUM (Jan. 24, 2018), <https://medium.com/@cehl/data-the-fuel-for-artificial-intelligence-ed90bf141372>.

95. Bernard Marr, *The Amazing Ways Tesla Is Using Artificial Intelligence and Big Data*, FORBES (Jan. 8, 2018, 12:28 AM), <https://www.forbes.com/sites/bernardmarr/2018/01/08/the-amazing-ways-tesla-is-using-artificial-intelligence-and-big-data/>.

96. *Background Note by the Secretariat*, *supra* note 32, at 5.

97. *See, e.g.*, Stucke & Grunes, *supra* note 33, at 8; Autorité de la Concurrence and Bundeskartellamt, *supra* note 52, at 11.

98. *Background Note by the Secretariat*, *supra* note 32, at 17.

in being akin to information—that has produced consequences across such a broad range of fields, including personal privacy, democracy, security, innovation stifling, hacking, political influence, and media. To put it into the context of the first historic network-effected monopoly, what we are seeing today would be something analogous to if the Bell Telephone Company had not only the monopoly on the physical telephone lines, but also on the recording and analysis of the conversations traveling through the lines, as well as control over 80% of the major newspapers—all while being the world’s largest company.⁹⁹ This highlights why data, with its likeness to information itself, can allow companies like Google and Facebook to create monopolies that are fundamentally different from our previous experience with network-effected monopolies like Microsoft Office.

When a data set becomes so vast and ubiquitous that it encompasses wide-ranging fields of human endeavor, then the controller of that data likewise becomes a powerful gatekeeper and influencer. When data is amassed—as Big Data is now—it is no longer something passive with discrete application, like a car, but something with all-inclusive utility. Rather, it transforms into knowledge—which can be political, personal, influential, private, or even confidential—and an essential element to innovation.

Not all data-opolies have as much power, value, and influence as Facebook and Google, however, because a data-opoly’s dominion depends on the type and variety of data. For example, Airbnb may essentially have a data-opoly over share accommodation, but it is simply not in a position to impact an election or act as a filter to our experience of the world. Similarly, Tesla may be in a data-driven network-effected market but, again, this data would seem to be limited to transport.

B. *Data Is Big*

In 2014, IBM estimated that 90% of the data in the world had been created in the previous two years alone.¹⁰⁰ Data is no longer concerned only with stock information such as a person’s name, email address, sex, and age. It now encompasses unstructured data from multiple, unlikely sources, including anything from dietary habits, heart rate, location,

99. Morgan Stanley estimated in 2016 that 85% of all online advertising expenditure would go into Google or Facebook. Jason Kint, *Google and Facebook Devour the Ad and Data Pie. Scraps for Everyone Else*, DIGITAL CONTENT NEXT (June 16, 2006), <https://digitalcontentnext.org/blog/2016/06/16/google-and-facebook-devour-the-ad-and-data-pie-scraps-for-everyone-else/>.

100. Todd Vare & Michael Mattioli, *Big Business, Big Government and Big Legal Questions*, MANAGING INTELL. PROP., Oct. 2014, at 46, <http://www.managingip.com/Article/3382483/Big-business-big-government-and-big-legal-questions.html>.

recycling habits, microenvironment rainfall, voting preference, when a car's thermostat turns on, to sexual pronouns used in speech. This vast unorganized data is then analyzed by sophisticated algorithms and artificial intelligence¹⁰¹ to find otherwise undiscoverable—and at times highly surprising¹⁰²—insights. Hagstrom writes that “[t]he combination of unconventional data sources, new problem-solving approaches, and the ability to use big data to access collective knowledge will enable organizations to devise innovative solutions to global problems.”¹⁰³

Big Data has been defined as information that is characterized by the four Vs: high volume, velocity, variety, and value.¹⁰⁴ It is now not so much the quality of the data that is important, but the sheer quantity. And over the past decade, “each ‘v’ has increased enormously.”¹⁰⁵ But the most noteworthy increase has been in value.¹⁰⁶

101. See Bernard Marr, *The Complete Beginner's Guide to Big Data Everyone Can Understand*, FORBES (Mar. 14, 2017), <https://www.forbes.com/sites/bernardmarr/2017/03/14/the-complete-beginners-guide-to-big-data-in-2017/#45d7d6e27365> (explaining how big data is collected and analyzed).

102. An example of a surprising find of big data was Walmart “finding that Strawberry pop-tarts sales increased by 7 times before a Hurricane. After Walmart identified this association between Hurricane and Strawberry pop-tarts through data mining, it places all the Strawberry pop-tarts at the checkouts before a hurricane.” *How Big Data Analysis Helped Increase Wal-Mart's Sales Turnover?*, DEZYRE, <https://www.dezyre.com/article/how-big-data-analysis-helped-increase-wal-marts-sales-turnover/109> (last updated Nov. 10, 2017).

103. Mikael Hagstrom, *How Big Data Can Help Solve the World's Woes*, WORLD ECON. FORUM (Oct. 25, 2015), www.weforum.org/agenda/2015/10/how-big-data-can-help-solve-the-worlds-woes/.

104. Analyst Douglas Laney first defined the three “v”s of volume, velocity and variety. Andrea De Mauro, Marco Greco, and Michele Grimaldi added the “value” component. See Andrea De Mauro et al., *A Formal Definition of Big Data Based on Its Essential Features*, 65 LIB. REV. 122, 130–31 (2016). The definition has been adopted recently by Stucke and Grunes, as well as by the OECD Competition Committee. STUCKE & GRUNES, *supra* note 37, at 16.

105. STUCKE & GRUNES, *supra* note 37, at 16.

106. Org. for Econ. Co-Operation and Dev. [OECD], *Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by “Big Data,”* at 12, DSTI/ICCP(2012)9/FINAL (Apr. 18, 2013), <https://www.oecd-ilibrary.org/docserver/5k47zw3fcp43-en.pdf?expires=1551680853&id=id&accname=guest&checksum=0971F2CD3870BD189D4B81DC55EFC985>. The OECD estimates that use of Big Data by 2020 could save \$500 billion USD in traffic congestion and fuel costs by use of mobile tracking; reduce the cost of carbon dioxide emissions by €79 billion by use of smart appliances; and in the U.S. medical sector, reduce medical errors, improve diagnosis, increase efficiency in management and pricing, foster R&D, and achieve other goals that would allow savings of about \$300 billion USD. *Id.* at 5.

Data is being called “the new oil.”¹⁰⁷ It is now “in every sector, in every economy, in every organization and user of digital technology.”¹⁰⁸ The more information, or Big Data, the better—those who possess such data can analyze it and make it into something useful.¹⁰⁹ The implications of Big Data are likely to appear in many various guises and its applications will be unusual and unpredictable. In this way, we would be better off to ensure adequate regulation of Big Data itself, not merely its discrete applications.

C. Facebook Case Study

Facebook has over two billion active users.¹¹⁰ The “Like” and “Share” buttons appear daily on almost 10 million websites, and every sixty seconds there are 510,000 comments posted, 293,000 statuses updated, and 136,000 photos uploaded.¹¹¹ When working with such numbers, even a slight tweak will enable seismic shifts. The data that Facebook collects and presents to its users has inherent political significance. Facebook is, in effect, the world’s largest media company. As former Gawker founder Nick Denton opines, “[t]he Silicon Valley . . . monopolies now have . . . more power than the [entire traditional] media industry.”¹¹²

Facebook’s capacity to affect users’ behavior in society is substantiated by its own research. Facebook funded a study that was later published in *Nature* during the 2010 United States congressional elections. By selectively giving some users an “I voted” button but not others, the study found that the presence of the button increased the total vote count in the election by 340,000 votes.¹¹³ In short, Facebook was actually able to subtly encourage 340,000 people to vote who otherwise would not have. In another experiment, Facebook researchers¹¹⁴ showed

107. *The New Oil: Data Is the World’s Most Valuable Resource*, AUSTL. (May 6, 2017, 1:00 AM) <https://www.theaustralian.com.au/news/inquirer/the-new-oil-data-is-the-worlds-most-valuable-resource/news-story/f386217a9c63ac5ee6e1473413e90bda>.

108. JAMES MANYIKA ET AL., *supra* note 93, at 2.

109. *See Data, Data Everywhere*, ECONOMIST, Feb. 27, 2010, at 3, <https://www.economist.com/special-report/2010/02/25/data-data-everywhere>.

110. FACEBOOK, INC., ANNUAL REPORT (FORM 10-K) 35 (2019), <https://www.sec.gov/Archives/edgar/data/1326801/000132680119000009/fb-12312018x10k.htm>.

111. *The Top 20 Valuable Facebook Statistics*, ZEPHORIA, <https://zephoria.com/top-15-valuable-facebook-statistics/> (last updated July 2019); *see also*, Press Release, Facebook, Facebook Reports Second Quarter 2017 Results (July 26, 2017), <https://investor.fb.com/investor-news/press-release-details/2017/Facebook-Reports-Second-Quarter-2017-Results/default.aspx>.

112. NOBODY SPEAK: TRIALS OF THE FREE PRESS (Netflix June 23, 2017) (quoting Nick Denton at 38:32).

113. Robert M. Bond et al., *A 61-Million-Person Experiment in Social Influence and Political Mobilization*, 489 NATURE 295, 297 (2012).

114. Adam D. I. Kramer et al., *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT’L ACAD. OF SCI. U.S. 87, 88 (2014).

how manipulating the Facebook news feeds could alter moods in users. Placing “positive emotional content” on users’ news feeds resulted in positive posts and, similarly, “negative emotional content” resulted in negative posts.¹¹⁵

Until recently, commentators questioned whether Facebook had the data to influence a U.S. election.¹¹⁶ But now that question seems to have been answered affirmatively in light of the Cambridge Analytica and Russian hacking scandals. Cambridge Analytica, a private data firm “funded and promoted by secretive [billionaire] Robert Mercer,”¹¹⁷ worked on advertising for the Trump presidential campaign.¹¹⁸ It used Facebook data, which it had bought from an application built by a Cambridge University academic, of 277,000 users who consented to their data being collected.¹¹⁹ However, Cambridge Analytica was able to mine and scrape data from friends of the original user so that, in the end, it had the personal data of 87 million people.¹²⁰ Using the insights extrapolated from the data, Cambridge Analytica microtargeted advertisements to swing voters, and all-told, the campaign launched 4,000 different ad campaigns and placed 1.4 billion web impressions.¹²¹ The way in which Cambridge Analytica was able to microtarget and influence voters using the data of 87 million people garnered much attention and criticism from the media, wider public, and commentators.¹²² Many believe it was instrumental in the success of the Trump campaign to the point where it seems to have disrupted democratic institutions.

115. The experiment is what prompted Clay Johnson, co-founder of the firm who ran the Obama online campaign, to postulate: “Could the CIA incite revolution in Sudan by pressuring Facebook to promote discontent? Should that be legal? Could Mark Zuckerberg swing an election . . . ? Should that be legal?” Robert Booth, *Facebook Reveals News Feed Experiment to Control Emotions*, GUARDIAN (June 29, 2014, 7:57 PM), <https://www.theguardian.com/technology/2014/jun/29/facebook-users-emotions-news-feeds>.

116. Michael Brand, *Can Facebook Influence an Election Result?*, ABC NEWS (Sept. 27, 2016), www.abc.net.au/news/2016-09-28/can-facebook-influence-an-election-result/7881660.

117. Sasha Issenberg, *Cruz-Connected Data Miner Aims to Get Inside U.S. Voters’ Heads*, BLOOMBERG (Nov. 12, 2015, 5:00 AM), <https://www.bloomberg.com/news/features/2015-11-12/is-the-republican-party-s-killer-data-app-for-real->.

118. Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

119. Olivia Solon, *Facebook Says Cambridge Analytica May Have Gained 37m More Users’ Data*, GUARDIAN (Apr. 5, 2018, 6:01 PM), <https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought>.

120. *Id.*; Mike Schroepfer, *An Update on Our Plans to Restrict Access on Facebook*, FACEBOOK (Apr. 4, 2018), <https://newsroom.fb.com/news/2018/04/restricting-data-access/>.

121. Dirk Helbing et al., *Will Democracy Survive Big Data and Artificial Intelligence?*, SCI. AM. (Feb. 25, 2017), <https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/>.

122. *Id.*

This informs us of another consequence of data monopolization. Even if we accept Facebook's claims that it has no agency¹²³ or political interest, its role as a centralized media outlet with deep and unique insights by virtue of data monopolization had the unintended consequence of enabling third parties to use that data for nefarious purposes. In response, CEO Mark Zuckerberg was called before the U.S. congressional committee. During the hearing, Zuckerberg admitted Facebook had failed in preventing Cambridge Analytica from gathering the personal information of users.¹²⁴

Facebook is promising to implement a policy that aims to more clearly explain the data it gathers on users, but not to actually change what information it collects and shares.¹²⁵ Again, while better privacy policies may prevent the same scenario, Facebook will continue to be the centralized commercial entity of the personal data of its billions of users.

The GDPR will similarly force Facebook to better outline its privacy policy. But for those who accept the policy, Facebook will still be vacuuming up data. Thus, Facebook's influence and power will likely be unaffected by the GDPR.

D. Google Case Study

To learn just about anything nowadays, the first instinct is to "Google it" because Google has become synonymous with knowledge. It is the portal through which we seek understanding. As the prism through which we discover and see much of the world, this places Google in a unique position of power and influence.

Google's mission is to "organize the world's information and make it universally accessible and useful."¹²⁶ Even without any suggestion¹²⁷ that

123. Facebook claims it has no agency. However, in 2016, Gizmodo broke the story that several former Facebook "news curators" admitted that they intentionally suppressed conservative new websites appearing in the "trending" news section despite the stories organically trending, and conversely, "injected" news articles they preferred into the trending news section. They were also instructed not to include news about Facebook itself. Michael Nunez, *Former Facebook Workers: We Routinely Suppressed Conservative News*, GIZMODO (May 10, 2016, 12:30 PM), www.gizmodo.com.au/2016/05/former-facebook-workers-we-routinely-suppressed-conservative-news/.

124. *Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?noredirect=on&utm_term=.a300d547415c.

125. *Facebook Says up to 87m People Affected in Cambridge Analytica Data-Mining Scandal*, ABC NEWS, <https://www.abc.net.au/news/2018-04-05/facebook-raises-cambridge-analytica-estimates/9620652> (last updated Apr. 4, 2018, 6:32 PM).

126. *About*, GOOGLE, www.google.com/intl/en/about/ (last visited Mar. 4, 2019).

127. One commentator noted we now need to use new language to describe the pervasiveness of Facebook and Google. Ellen P. Goodman & Julia Powles, *Facebook and Google: Most Powerful and Secretive Empires We've Ever Known*, GUARDIAN (Sept. 28, 2016, 3:00 PM),

Google aims to present this information and data in anything other than a neutral portal, acting as a gatekeeper places it in a perilous spot. And while its famous motto is “Don’t be evil,”¹²⁸ it remains a commercial enterprise with responsibilities to shareholders to maximize profits. Google has been known to bias their search results to push its own products ahead of competitors’ products. In a leaked 2012 staff report¹²⁹ about the dominance of Google in online searches, the FTC found that Google was giving preference to its own products and had “adopted a strategy of demoting or refusing to display, links to certain vertical websites in highly commercial categories.”¹³⁰ Nevertheless, the FTC decided not to pursue the matter at the time.¹³¹

Google has a “God’s eye view,” as the data it collects provides Google with information that it¹³² then uses to quickly spot competitor trends and either acquire them or out-compete them. Many believe that AI is the next big application of Big Data in the future. But Google already has that covered, too. It has the largest number of AI experts in the world and has invested £400 million into DeepMind,¹³³ a program that aims to “solve intelligence”—a nice addition to go alongside hundreds of other start-ups Google has bought.¹³⁴ Last year, at the launch of its Pixel 2 phone in San Francisco, Google announced its plans to transition from a “mobile-first”

<https://www.theguardian.com/technology/2016/sep/28/google-facebook-powerful-secretive-empire-transparency> (“Google is not an ‘engine’ that simply drives us to an objectively correct destination . . . Facebook is not merely a ‘network’ for connection, like the old phone network or electrical grid, as if it had no agency . . . These are not mere ‘edge providers,’ peripheral to infrastructure, or mere ‘applications’ that we can select or refuse.”).

128. Julian Assange, Opinion, *The Banality of “Don’t Be Evil,”* N.Y. TIMES (June 1, 2013), <https://www.nytimes.com/2013/06/02/opinion/sunday/the-banality-of-googles-dont-be-evil.html>; Kate Conger, *Google Removes “Don’t Be Evil” Clause From Its Code of Conduct*, GIZMODO (May 18, 2018, 5:31 PM), <https://gizmodo.com/google-removes-nearly-all-mentions-of-dont-be-evil-from-1826153393>.

129. Brody Mullins et al., *Inside the U.S. Antitrust Probe of Google*, WALL ST. J. (Mar. 19, 2015, 7:38 PM), <https://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274>.

130. *Excerpts from FTC Google Report*, WALL ST. J. (Mar. 19, 2015, 6:30 PM), graphics.wsj.com/ftc-google-report/.

131. Press Release, Federal Trade Commission, Privacy Settlement is the Largest FTC Penalty Ever for Violation of a Commission Order (Aug. 9, 2012), www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

132. ECONOMIST, *supra* note 10.

133. Sam Shead, *The Founders of Google DeepMind Are Investing in a Startup That Lets You Talk to a Doctor Through Your Smartphone*, BUS. INSIDER (Jan. 14, 2016, 3:10 AM), www.businessinsider.com.au/deepmind-cofounders-invest-in-babylon-health-2016-1.

134. Jennifer Elias, *Google’s Acquisitions Are in the Spotlight 15 Years After It Went Public*, CNBC, <https://www.cnbc.com/2019/08/19/googles-best-and-worst-acquisitions-are-in-the-spotlight-15-years-later.html> (last updated Aug. 19, 2019, 12:20 PM).

business to an “AI-first” business.¹³⁵ If AI and the data it runs on is set to be the future of innovation, then Google is in the lead.

Like all large companies, Google also has more traditional power. According to Professor Reich, “Google is now among the largest corporate lobbyists in the United States. Around the time of the [FTC] investigation the company poured money into influencing both the commissioners and the commission’s congressional overseers.”¹³⁶

Another example of the power of Big Data is Google’s ability to predict influenza epidemics. By analyzing user searches for flu symptoms, it is able to predict outbreaks. There is even one report that Google was able to predict regional outbreaks of the flu up to ten days before the outbreaks were reported by the Center for Disease Control and Prevention in the U.S.¹³⁷ Google did not start out in the business of epidemiology. However, data enabled it to be a possible world leader in the field.

Google has found itself in this powerful data monopoly primarily on the back of a single innovation twenty years ago. However, it has no obligation or incentive to give access to its data, nor to explain how its algorithms function. The data we provide Google, and also Facebook, is extremely personal. In some way, each probably knows more about us than all our friends combined. Google knows what we say (Gmail), watch (YouTube), think (Google search), look like (Google Photos), buy (Google Wallet), where we drive (Maps), who we meet and where (Google Calendar), and it only just stopped short of wanting a live stream of our entire lives (Google Glass). This personal and sensitive aspect further illustrates the special nature of data as a commodity that makes it unlike any previous commodity controlled by centralized, commercial entities.

E. *Data as Something More*

These two case studies highlight the dark side to a data-opoly—the consequences of the monopolistic data control that Google and Facebook have over personal information, news media, information generally, and collective knowledge—to which neither competition nor consumer laws speak directly. To the civil rights advocate, the problem is that the personal data of the individual is being misused. To the economist, however, the problem is one of monopolistic prices and inferior goods.

135. Peter Marks, *Pixel 2: The Smartphone Age Is Over and Google Thinks AI Is Next*, ABC NEWS (Oct. 5, 2017, 3:19 AM), <https://www.abc.net.au/news/2017-10-05/google-pixel-2-heralds-the-ai-age/9018636>.

136. Reich, *supra* note 12.

137. Stucke & Grunes, *supra* note **Error! Bookmark not defined.**, at 7; *see also* Miguel Helft, *Google Uses Searches to Track Flu’s Spread*, N.Y. TIMES (Nov. 11, 2008), <https://www.nytimes.com/2008/11/12/technology/internet/12flu.html>.

Thus, the economic analysis is skewed towards the economic outcomes of data-opolies and how competition laws need to be re-tooled to better fit the anti-competitive nature of a monopoly when the subject matter is data. While higher prices and personal data privacy are serious, rectifying them will not resolve the problem of the power and control exercised by enterprises like Facebook and Google. At the other end, those in the mainstream and the more specialized financial press have been aware of the power and control issues of Facebook and Google, but have been largely unable to pinpoint the means through which the centralization of power was occurring: the data-opoly.

IV. SOLUTIONS

A. *Changing Our View of Data*

The value of digital technology, and Big Data in particular, as being amongst the world's greatest tools in a number of respects is only recently being discussed. Hagstrom predicts that "if the universe of data were suddenly made available, it would unleash the creativity of problem-solvers to combine different data sets—public and private—to develop innovative solutions to innumerable challenges."¹³⁸

Perhaps it is not surprising, then, that a likely reason we are not rectifying the quasi-monopoly control of data is because we have yet to recognize its intrinsic value. Instead, we have focused upon the downstream glitches—until now. What follows are some suggestions for possible solutions and are flagged here for further discussion. The common thread of these solutions is changing how we view data.

B. *Time Limiting Data*

One possible solution is the implementation of a mechanism—legal or computational—that imposes a time limit for preventing access to data. Collected data could be given a limited term, and once expired, the controller of the data would be compelled to make the data available for public consumption. So, for example, when a timestamped block of data reaches a certain maturity, say five years,¹³⁹ and if there are no privacy or security issues, then it is automatically rendered open access. This could act as the blunt tool that ultimately prevents companies from monopolizing their useful data.

138. Hagstrom, *supra* note 103.

139. This would not solve the problem of monopolized Big Data that has its value in its "velocity," such as traffic data. However, much of the big data collected now will still have relevance in 5 years—for example, data about the human body.

This idea is, of course, borrowed from the current regime that regulates data's first cousin, intellectual property.¹⁴⁰ Ever since its inception, intellectual property has experienced great difficulty in balancing the tension between encouraging innovation and preventing abuse of monopolistic power.¹⁴¹ This is analogous to the tension inherent to data-opolies. We recognize that data is useful and so on one hand we want to encourage its creation and collection, while on the other hand we want to allow access and disclosure of that data to the public. Currently, however, there is little reason for a company to share its data.¹⁴² Such a shift from privately controlled data to open access will subject data-opolies to the self-limiting mechanism in intellectual property: its term.

C. *Thinking of Data as a Commodity, Labor, or a Human Right*

Currently, the data-opolies do not offer their data for sale.¹⁴³ Amazon, Facebook and Google explicitly state they do not sell their users' data.¹⁴⁴ Instead, data is kept private for the benefit of the data-opolies. However, if a market were established for data as a commodity, then data would no longer be locked away but could be traded on the free market and applied where the market determined there was a need.

140. Graef, *supra* note 51, at 6 (finding that data and intellectual property are non-rivalrous goods).

141. This balance finds expression in the "bargain" of the patent regime. *See* *Teva Canada Ltd. v. Pfizer Canada Inc.*, [2012] 3 S.C.R. 625 (Can.) ("The patent system is based on a 'bargain,' or quid pro quo: the inventor is granted exclusive rights in a new and useful invention for a limited period in exchange for disclosure of the invention so that society can benefit from this knowledge. This is the basic policy rationale underlying the Act. The patent bargain encourages innovation and advances science and technology.").

142. *Background Note by the Secretariat*, *supra* note 32, at 28. The OECD report identified this option but went on to say that requiring a company to share data would be an extreme remedy, only to be used where no less intrusive alternatives existed. OECD *Executive Summary*, *supra* note 69, at 4. A very different view is expressed by Larry Lessig when talking about intellectual property and our fascination with absolute control, however. Lawrence Lessig, *Intellectual Property and Code*, 11 J. CIV. RTS. & ECON. DEV. 635, 638 (1996) ("[W]hile we protect real property to protect the owner from harm, we protect intellectual property to provide the owner sufficient incentive to produce such property. 'Sufficient incentive,' however, is something less than 'perfect control.'"). The Productivity Commission observed the same problem in the context of confidential pharmaceutical data. *See* AUSTRALIAN GOVERNMENT PRODUCTIVITY COMMISSION, INQUIRY REPORT NO. 78: INTELLECTUAL PROPERTY ARRANGEMENTS OVERVIEW & RECOMMENDATIONS 19 (2016).

143. Twitter is an exception. *See* Selina Wang, *Twitter Sold Data Access to Cambridge Analytica-Linked Researcher*, BLOOMBERG (Apr. 29, 2018, 2:26 PM), <https://www.bloomberg.com/news/articles/2018-04-29/twitter-sold-cambridge-analytica-researcher-public-data-access>.

144. *See Amazon Privacy Notice*, AMAZON, <https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010> (last updated Aug. 29, 2017); *Does Facebook Sell My Information?*, FACEBOOK, <https://www.facebook.com/help/152637448140583> (last visited Aug.

In a similar way, it is also possible to view data as the labor of the user who provided it. According to researchers studying a system for measuring the value of individual data contributions, “[d]ata is labour.”¹⁴⁵

In some scenarios, in times of a humanitarian crisis for example, data is also starting to be understood as a human right.¹⁴⁶ Elevating data to this position of reverence would change the mindset of both society and the data-opolies. Such a shift in how data is viewed would encourage data reform.

D. Blockchain Technology

The answer may not lie solely in the traditional legal frameworks, however. As the volume of data collected surges and the nature of data changes—as it is derived from increasingly complex and extensive global networks—it appears that building an automated computational system to regulate the data itself would be adequate to curb the effects of data-opolies.

Blockchain is a very recent digital technology that employs an “open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way.”¹⁴⁷ The transactions are recorded in data sets, called blocks, which are linked to each other by unique hash codes, generated and timestamped by the data block itself.¹⁴⁸ Blockchain technology is supremely well suited¹⁴⁹ to solve the problem of monopolization of Big Data: (1) it is by definition decentralized and distributed;¹⁵⁰ (2) it runs by unsupervised automated code—the best way

22, 2019); *Privacy*, GOOGLE, <https://support.google.com/googlecloud/answer/6056650?hl=en> (last visited Aug. 22, 2019).

145. See generally E. Glen Weyl, et al., *Should We Treat Data as Labor? Moving Beyond “Free,”* 108 AM. ECON. ASS’N PAPERS & PROC. 38 (2018).

146. See generally FAINE GREENWOOD ET AL., HARV. HUMANITARIAN INITIATIVE, *THE SIGNAL CODE: A HUMAN RIGHTS APPROACH TO INFORMATION DURING CRISIS* (2017), https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf.

147. Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV., Jan.–Feb. 2017, at 118. <https://hbr.org/2017/01/the-truth-about-blockchain>.

148. See ARVIND NARAYANAN ET AL., *BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES: A COMPREHENSIVE INTRODUCTION* 11–12 (2016).

149. At its heart, blockchain technology provides a system whereby people and agents can interact in a trusted and virtually frictionless transactional system. Although a very new technology, it is already recognized—even hyped—to be particularly applicable for use in currency, voting, data privacy management, and legal transaction of property. See *Distributed Organization*, SYS. ACAD., <http://complexitylabs.io/blockchain-distributed-organization/> (last visited Aug. 22, 2019).

150. Blockchain technology distributes the load of data storage, thus dispensing of the previously inhibitory capital costs for newcomers. See *id.*

to regulate something of the massive scale of Big Data;¹⁵¹ (3) it deals with data, which is precisely the subject of the monopolization; and (4) it can employ token economics¹⁵² and smart contracts.¹⁵³

Currently, most digital platforms we use are within the Web 2.0 framework which is comprised of companies such as Google and Facebook vacuuming up any and all data we generate and storing them on centrally controlled data servers. However, researchers and designers anticipate Web 3.0, where digital platforms such as Ethereum¹⁵⁴—which are open-sourced and decentralized—can be used to run platforms previously only provided by centralized businesses. This will also solve the barrier of large data storing infrastructure.¹⁵⁵ The large servers needed to physically hold the data, and the human experts and development required to undertake the “deep” analysis is costly.¹⁵⁶ For example, Microsoft considered it necessary to outlay \$4.5 billion USD into “developing its algorithms and building the physical capacity necessary to operate Bing”¹⁵⁷ in its attempt to compete in the search engine market.

151. The scale of the big data is so great that the execution, enforcement, and administration of regulations can only be realistically performed by unsupervised computational regulation, whether it be using blockchain or artificial intelligence. It is simply impossible for a human to comb over such large and fluctuating data to determine whether it meets the definition of monopolized Big Data.

152. If a market was established for data as a commodity, then it could be traded and applied where the market determined there was need. The blockchain could use token economics to attempt to solve this using traditional economics. However, an added benefit of token economics is that of a multivalued and fully fungible economy, allowing us to represent value otherwise not well captured by traditional economics such as environmental or humanitarian value.

153. Smart contracts are the second generation blockchain. The additional feature is that the blockchain also contains executable code on the blockchain in this same distributed way. The smart contract is both defined and enforced by the code, without discretion. So more than just a passive distributed ledger, second generation blockchains with smart contracts can perform contractual obligations. For example, a smart contract can issue the access code for a house once the accommodation fee is paid.

154. Ethereum is an open-source public blockchain distributed computer platform featuring smart contracts. It was only recently created in a 2013 white paper, then went live one year later. *Who Created Ethereum?*, BITCOIN MAG., <https://bitcoinmagazine.com/guides/who-created-ethereum> (last visited Aug. 22, 2019).

155. Data storage infrastructure involves significant costs. *Background Note by the Secretariat*, *supra* note 32, at 11 (“[T]he information technologies required to store and process the data can be very costly, involving vast data centres, servers, data-analytical software, internet connections with advanced firewalls and expensive human resources, such as computer scientists and programmers.”).

156. In 2016, Amazon, Google and Microsoft spent \$32 billion USD in capital expenditure and capital leases. AUSTL., *supra* note 107.

157. *The FTC Report on Google’s Business Practices*, WALL ST. J. (Mar. 24, 2015, 7:40 PM), <http://graphics.wsj.com/google-ftc-report/> (stating that Microsoft invested over \$4.5 billion into developing Bing on page 76 of the memorandum prepared by staffers at the Federal Trade Commission); Stucke & Grunes, *supra* note 33, at 5.

Accordingly, under Web 3.0, the data exhaust generated by users is no longer controlled by a centralized, commercial entity. Instead, the massive amounts of data may be managed by the user or society collectively. The problem then is no longer one of accessing data that is useful, but what we do with that data. This provides a huge opportunity to employ blockchain technology to very efficiently manage the full potential of Big Data to change our lives.

CONCLUSION

The creation of digital powerhouses such as Google, Amazon, Apple, Microsoft, and Facebook has been largely due to a data-driven network effect. Traditionally, mitigating network-effected markets has been problematic. Mitigation has proved even more difficult in the case of data monopolies because the data itself is not openly traded.

More consequential, however, is that data is unlike other goods or services that have been monopolized previously. Data has inherent value. As more of our activities are being digitized, the Big Data being generated is proving to be a powerful tool across fields as varied as curing disease, feeding the hungry, reducing gender inequality, strengthening national security, and improving environmental and disaster responses. Thus, when large volumes of data are marshalled and monopolized, there is more at stake than simply higher prices and poor privacy policies.

The advent of the internet and digital technology is likely to be the defining feature of the history of humankind in this century. Its promise is great and so too is its potential for misuse. If data is to be the driving force behind this new technology, we must manage it well with the implementation of new laws for the purpose of preventing the misuse of data. Alternatively, we could possibly even look to digital technology itself to build an automated computational system of regulation.

THE PSYCHOLOGICAL AND VIRTUAL SIEGE OF LOOT BOXES

*Elpidio K. Cruz**

I. AN UNPRECEDENTED LANDSCAPE.....	215
II. WHAT ARE LOOT BOXES AND WHAT DO THEY DO?.....	217
III. CONCLUSION	227

I. AN UNPRECEDENTED LANDSCAPE

When you think of sports, how do you imagine where the athletes play? The lushest grass you’ve ever seen? An unending blue sky? None of the above? If you are watching the game from the comfort of your home, what channel is broadcasting it? CBS? ESPN? Now compare your answer to an answer you would have given a few years ago. Any similarities?

Technology is changing rapidly, with the video entertainment world right behind it. Virtual reality, biometric scanning, and all sorts of other developments are changing the way the world views technology. Who would have thought that you could walk around your neighborhood and catch Pokemon?¹

One change that was unlikely to be predicted was the rise of eSports.² An eSport is an online, multiplayer video game played competitively that spectators can view live.³ Simply put, these games take a sport and make an electronic version of it. People are now able to play soccer, football,

* J.D., University of Florida, Levin College of Law (2019); B.A., University of Florida (2016). Thank you to my family, friends, classmates, and everyone that has provided me with guidance and advice for improvement. Secondly, thank you to the Journal of Technology Law and Policy for selecting me for publication.

1. POKEMON GO, <http://origin.pokemongo.com/> (last visited Oct. 24, 2018). This game is able to take advantage of augmented reality to place a virtual object at a fixed spot in the real world. It was an alarming success with \$600 million in revenue within the first three months. Joon Ian Wong, *We Finally Know How Much Nintendo Made from Pokemon Go*, QUARTZ (Oct. 26, 2016), <https://qz.com/819677/nintendo-pokemon-go-profits-we-finally-know-how-much-nintendo-made-from-pokemon-go/>.

2. The eSport industry has exploded within the past five years. In 2014, it was reported that over 200 million individuals viewed or participated in eSports, 89 million of whom were “frequent viewers” or “enthusiasts.” Additionally, while the field has been traditionally male dominated, studies show that 38%–44% of American eSports fans are women. One of the most exciting parts is that these numbers will only continue to grow. See Ben Casselman, *Resistance Is Futile: eSports Is Massive . . . and Growing*, ESPN (May 22, 2015), http://www.espn.co.uk/espn/story/_/id/13059210/esports-massive-industry-growing.

3. *E-sport*, LEXICO, <https://www.lexico.com/en/definition/e-sport> (last visited June 24, 2019).

and basketball without ever having to leave their couches.⁴ The most exciting part is that these people can compete with other players around the world, all with the push of a button. These competitions can occur at a place in town or entirely through the internet. Such accessibility allows massive tournaments to take place with grand prizes and relatively low, if any, location costs.⁵ In fact, the winner of the FIFA Interactive World Cup 2017, an eSports soccer tournament, was awarded \$200,000 for his victory.⁶

The debut of the first ever FIFA eWorld Cup took place in 2018.⁷ For this tournament alone, 20 million individuals from around the world competed—only thirty-two were admitted into the tournament.⁸ The qualifiers were from various countries, including the United States, France, Germany, and Saudi Arabia.⁹

Throughout online gaming, leagues are developing where players compete against each other. Most games use “rankings” to compare their players globally.¹⁰ Now, what happens when you create a tournament for teams within these leagues?

Consider League of Legends, a free multiplayer online battle arena game that places individuals on teams to fight against each other.¹¹ It requires strategy, patience, and teamwork. It also provides an opportunity

4. For example, EA Sports Inc. has developed sports games, including FIFA, Madden, and NBA LIVE, that simulate soccer, football, and basketball, respectively. See EASPORTS, <https://www.easports.com> (last visited June 24, 2019).

5. The World Championship “Natural Selection II” tournament cost \$67,443 to operate. For larger tournaments, companies spend millions. See Hamza Aziz, *So How Much Does It Cost to Host an eSports Competition Anyway?*, DESTRUCTOID (Mar. 11, 2014, 4:00 PM), <https://www.destructoid.com/so-how-much-does-it-cost-to-host-an-esports-competition-anyway--271749.phtml>. However, this cost remains substantially lower than the largest live sporting events such as the Super Bowl, which raised \$53 million to spend on the event. Eric Roper, *Cost of Hosting Super Bowl Remains Unclear, But NFL Demands a Lot*, STAR TRIB. (Feb. 3, 2018, 4:01 PM), <http://www.startribune.com/cost-of-hosting-super-bowl-remains-unclear-but-nfl-demands-a-lot/472512273/>.

6. Steven Jurek, *Gorilla Wins \$200,000 FIFA Interactive World Cup 2017*, DOT ESPORTS (Aug. 18, 2017, 2:45 PM), <https://dotsports.com/general/news/gorilla-fifa-fiwc-2017-16757>. The eWorld Cup replaced the Interactive World Cup in 2018. *FIFA eWorld Cup 2018*, FIFA, <https://origin.fifa.com/fifaeworldcup/faq/index.html> (last visited Apr. 21, 2019).

7. *Id.*

8. *First 16 Qualifiers for the FIFA eWorld Cup Grand Final 2018*, FIFA (May 30, 2018), <https://www.fifa.com/news/wed-305-first-16-qualifiers-for-the-fifa-eworld-cup-grand-final-2018-2951878>.

9. *Id.*

10. *Id.*

11. *What Is League of Legends?*, LEAGUE OF LEGENDS, <https://na.leagueoflegends.com/en/game-info/get-started/what-is-lol/> (last visited Apr. 21, 2019).

to generate income through sponsorship, product sales, and sports gambling.¹²

Certain game mechanics take advantage of a system of in-game items that allow players to customize their avatar. For example, in games such as Fortnite, there are different items or skins that a player may use.¹³ The items may be earned either through accomplishments while playing or purchased with virtual currency through a randomized in-game mechanic. Players, by merely using the items in-game, generates free product placement. Further, the limited-edition nature of these items creates an environment where players will spend real money to acquire such limited edition or customized items.¹⁴

While normally not an issue, what happens when these items are purchased by minors? Children are known to be susceptible to the “I have to have it because everyone else has one” mindset.¹⁵ When children obtain these items through a system, much like a virtual “in-game casino,” certain legal issues arise. This Note will examine the development of in-game purchases in the video game industry.

II. WHAT ARE LOOT BOXES AND WHAT DO THEY DO?

Most video games allow the use of fiat currency to acquire objects and assistance within the video game.¹⁶ The most common forms of obtaining these perks are the acquisition of loot boxes and micro-transactions.¹⁷ A

12. League of Legends is considered a \$1 billion business. Edgar Alvarez, *The Traditional Sports World Is Taking eSports into the Mainstream*, ENGADGET (July 21, 2017), <https://www.engadget.com/2017/07/21/how-the-traditional-sports-world-is-embracing-esports/>. In the eSports betting market, League of Legends maintains roughly 38% of the total game betting volume. *Esports Betting—Overview of the Esports Gambling Vertical*, LEGAL SPORTS REP., <https://www.legalsportsreport.com/esports-betting/> (last updated May 10, 2018). The eSports betting industry is also capitalizing on the development of blockchain. One company in particular is striving to develop a betting company that operates using only blockchain technology. Stefanie Fogel, *Esports Gets Legalized Sports Gambling*, VARIETY (Oct. 24, 2018, 2:33 PM), <https://variety.com/2018/gaming/news/unikrn-gets-wagering-license-for-esports-betting-1202992593/>.

13. *All Skins*, SKIN-TRACKER, <https://skin-tracker.com/fortnite/skins> (last visited Apr. 21, 2019).

14. See Kellen Beck, *‘Counter Strike’ Skin Creators Are Making at Least 6 Figures a Year*, MASHABLE (May 2, 2017), <https://mashable.com/2017/05/02/counter-strike-skins/#N0COz18laPq9>.

15. Emily Sohn, *Why Do Children Love Those Fad Toys So?*, NPR (May 10, 2017, 12:25 PM), <https://www.npr.org/sections/health-shots/2017/05/10/527769527/why-do-children-love-those-fad-toys-so>.

16. Prateek Agarwal, *Economics of Microtransactions in Video Games*, INTELLIGENT ECONOMIST, <https://www.intelligenteconomist.com/economics-of-microtransactions/> (last updated Apr. 10, 2019).

17. *Id.*

micro-transaction is generally an in-game purchase that allows the player to access additional content.¹⁸ That content may assist a user in completing objectives that would be possible to complete without the additional purchase, but with more difficulty.¹⁹

A loot box, which contains an unknown item or items, is given to players as a prize.²⁰ Loot boxes do not create a direct financial incentive, but are instead a “game of chance.”²¹ If a player is lucky enough to get the item he or she wants—great! If not, then the player is stuck with undesirable junk items. Players want the most unique and rare loot to show off to their friends or their competitors.²² Purchasing a loot box is usually cheaper than purchasing rare items directly, and sometimes an item is only obtainable through the acquisition of a loot box.²³ This creates an incentive for players to try to open as many loot boxes as possible to increase their odds of obtaining the most enticing loot. The loot could be simply aesthetic, such as a new costume, or something more substantial, such as a valuable weapon.²⁴ With these new items, a player may perform better than competitors in the game, which then encourages other players to open boxes to even the playing field.

Some games, such as *Overwatch* or *League of Legends*, allow players to earn the boxes through in-game performance or through special giveaways only.²⁵ As noted above, those games also allow players to acquire loot boxes with fiat currency.²⁶ When fiat currency is involved, it is difficult to ignore the similarities between loot boxes and real-world

18. Chelsea King, Note, *Forcing Players to Walk the Plank: Why End User License Agreements Improperly Control Players' Rights Regarding Microtransactions in Video Games*, 58 WM. & MARY L. REV. 1365, 1367 (2017).

19. S. 1629, 116th Cong. (2019), <https://www.hawley.senate.gov/sites/default/files/2019-05/Loot-Box-Bill-Text.pdf> (defining pay-to-win microtransactions).

20. Keza MacDonald, *Belgium Is Right to Class Video Game Loot Boxes as Child Gambling*, GUARDIAN, <https://www.theguardian.com/games/2018/apr/26/belgium-is-right-to-legislate-against-video-game-loot-boxes> (last updated Aug. 15, 2018, 7:48 PM).

21. *Id.*

22. See Owen S. Good, *ESRB's New 'In-Game Purchases' Label, Explained*, POLYGON (Feb. 28, 2018, 8:25 AM), <https://www.polygon.com/2018/2/28/17059936/esrb-loot-crates-loot-boxes-label-in-game-purchases> (noting some players' belief that loot boxes are necessary to be successful in a game).

23. See Daniel Friedman, *Want Overwatch to Get Rid of Loot Boxes? It Might Get More Expensive*, POLYGON (Sept. 5, 2018, 2:00 PM), <https://www.polygon.com/2018/9/5/17822966/overwatch-loot-boxes-skins-events>.

24. Jason M. Bailey, *A Video Game 'Loot Box' Offers Coveted Rewards, But Is It Gambling?*, N.Y. TIMES (Apr. 24, 2018), <https://www.nytimes.com/2018/04/24/business/loot-boxes-video-games.html>.

25. See *id.*; Friedman, *supra* note 23.

26. Heather Alexandra, *Riot Discloses Loot Box Odds for League of Legends*, KOTAKU (Feb. 23, 2018, 3:00 PM), <https://kotaku.com/riot-discloses-loot-box-odds-for-league-of-legends-1823275409>.

gambling.²⁷ A loot box operates like a slot machine: a player inserts a coin and receives a random prize.²⁸ One could argue the mechanics of loot boxes are more akin to the toy dispensing machines located in local supermarkets. Much like loot boxes, those machines are usually catered to children. A child puts a quarter in the slot, turns it, receives a random toy from inside, and is usually disappointed with the result.

As demonstrated by world leaders, the industry and players are unsure how to categorize a loot box.²⁹ In this area of uncertainty, the only sure thing is that the issue is coming to the forefront of the industry's attention.³⁰ Moreover, loot boxes—and their similarity to gambling—has even gained the attention of state legislators. Some states have determined that the loot box system is gambling and must be regulated in the same way as other gambling machines. For example, Minnesota plans to restrict the sale of games with loot box mechanics to persons 18 years old or older.³¹ Further, Minnesota would require that those games be sold with a warning about the presence of the loot box mechanic.³² Other states following suit are California, Hawaii, Indiana, and Washington State.³³

The issue is also being considered in Australia: the Australian Environment and Communications Reference Committee recommended that loot boxes be restricted to individuals over 18 years old.³⁴ However, no Australian legislation has been enacted.³⁵ Other countries around the world are also investigating the issue of whether or not loot boxes are a form of gambling.³⁶ Japan has addressed the issue by banning a specific

27. Nick Santangelo, *Ireland Backs Down from Labeling Loot Boxes as Gambling*, IGN (Oct. 1, 2018, 7:34 AM), <https://www.ign.com/articles/2018/10/01/ireland-backs-down-from-labeling-loot-boxes-as-gambling> (“Where a game offers the possibility of placing a bet . . . for financial reward within the game, then, in my view it must be licensed as a gambling product.”).

28. MacDonald, *supra* note 20.

29. *See id.* (noting that Belgium found loot boxes violated gambling legislation); Santangelo, *supra* note 27 (noting that Ireland did not classify loot boxes as gambling).

30. MacDonald, *supra* note 20 (noting that the loot box mechanic created concern among players and politicians).

31. 2018 Minn. Laws 8385, https://www.revisor.mn.gov/bills/text.php?number=SF4042&version=latest&session=ls90&session_year=2018&session_number=0.

32. *Id.*

33. Bailey, *supra* note 24; *see also* Alexandra, *supra* note 26 (describing Hawaii's view on the matter).

34. Shaun Prescott, *Loot Boxes Are “Psychologically Akin to Gambling,” According to Australian Study*, PC GAMER (Sept. 18, 2018), <https://www.pcgamer.com/loot-boxes-are-psychologically-akin-to-gambling-according-to-australian-study/>.

35. Ryan Whitwam, *Study: Loot Boxes Are ‘Psychologically Akin to Gambling,’* EXTREMETECH (Sept. 18, 2018, 4:02 PM), <https://www.extremetech.com/gaming/277317-study-loot-boxes-are-psychologically-akin-to-gambling?source=gaming>.

36. *Id.*

loot box mechanic that required excessive spending for a small chance of a reward.³⁷ China has also taken steps to create legislation to regulate loot boxes.³⁸ Moreover, Belgium and the Netherlands have indicated that they believe loot boxes are gambling.³⁹ On the other hand, the United Kingdom and New Zealand have stated that loot boxes are not considered gambling.⁴⁰

One collaborative effort is the Gaming Regulators European Forum (GREF). Its mission is to gather European gaming regulators to discuss ongoing developments in the gaming industry, including gambling.⁴¹ The GREF has produced a declaration that discusses the “blurring of lines between gambling and other forms of digital entertainment such as video gaming.”⁴² The declaration was signed by sixteen gambling regulators total.⁴³ Unfortunately, the signing of the declaration does not establish a legal precedent that meaningfully regulates loot boxes.⁴⁴ Despite the tide seeming to roll in the direction of regulation, one video game publisher has taken a stance against the anti-loot box legislation abroad.⁴⁵

EA Sports uses a loot box mechanic.⁴⁶ Issues arose for EA when the Belgian gaming commission determined that loot boxes were illegal.⁴⁷ While other publishers removed the loot box option from their games, EA decided to keep the mechanic in the FIFA video game.⁴⁸ No legal

37. Sam Nordmark, *Legislators Are Targeting Loot Boxes, Here's Why*, DOT ESPORTS (Oct. 20, 2018, 10:26 AM), <https://dotesports.com/business/news/legislators-are-targeting-loot-boxes-heres-why%E2%82%AC>.

38. *Id.*

39. *Id.*

40. See Jessie Wade, *European and U.S. Gambling Regulators Sign Agreement to Tackle Gambling in Games*, IGN (Sept. 17, 2018, 9:54 PM), <https://www.ign.com/articles/2018/09/17/european-and-us-gambling-regulators-sign-agreement-to-tackle-gambling-in-games> (citing the Chief Executive and signatory for the UK gambling commission).

41. *Main Objectives*, GAMING REGULATORS EUR. F., <https://www.gref.net/about-grefexecutive-board/main-objectives/> (last visited Apr. 22, 2019).

42. *Declaration of Gambling Regulators on Their Concerns Related to the Blurring of Lines Between Gambling and Gaming*, GAMBLING COMM'N (Sept. 17, 2018), <https://www.gamblingcommission.gov.uk/PDF/International-gaming-and-gambling-declaration-2018.pdf>.

43. The declaration reflects the shared concerns of its signatories, which include Latvia, Czech Republic, Isle of Man, French, Spain, Malta, Jersey, Gibraltar, Ireland, Portugal, Norway, Netherlands, United Kingdom, Poland, Austria, and Washington State. See *id.*

44. See Santangelo, *supra* note 27 (providing the statement of the Ireland Department of Justice Minister of State, David Stanton).

45. See Ryan Whitman, *EA May Get Sued Over FIFA Loot Crates in Belgium*, EXTREMETECH (Sept. 11, 2018, 3:38 PM), <https://www.extremetech.com/gaming/276779-ea-may-get-sued-over-fifa-loot-crates-in-belgium>.

46. *Id.*

47. *Id.*

48. *Id.*

action has been taken yet, but Belgium's prosecutor is currently investigating EA to determine whether there is a case.⁴⁹ The outcome of this case will certainly have a global effect since it will be one of the first loot box legal battles.⁵⁰

At the time of this Note, the industry has not challenged the legality of any state legislation passed in the United States.⁵¹ Video Game Industry representatives assert that loot boxes are not gambling. In support, they propose two arguments: (1) each time a player purchases a loot box, he or she receives something in return, and (2) no player is required to buy or use a loot box to play the game.⁵² While such considerations should grant pause in the minds of legislators and readers, those two arguments are not sufficient to distinguish the loot box from gambling.⁵³

Beginning with the first argument, simply receiving something in return does not by itself create a distinction. Rather, the proper distinction should focus on the concept of consideration, which serves as the foundation of contract law.⁵⁴ The loot box mechanic thus falls under the auspice of contract law and it should be treated as a contract. Is the player always receiving something of equal or similar value in exchange for his or her money? Is there a return promise? In the case of loot boxes, the answer is most likely no. Consider the slot machine: players insert a dollar and receive something in return, even if it is sometimes only twenty-five cents. Similarly, the selection of a loot box is entirely random and involves nothing but a computer code.⁵⁵ Players may receive items

49. *Id.* See also Jessie Wade, *EA Reportedly Under Criminal Investigation in Belgium for Refusal to Modify FIFA Loot Boxes*, IGN (Sept. 11, 2018, 10:27 AM), <https://www.ign.com/articles/2018/09/11/ea-reportedly-under-criminal-investigation-in-belgium-for-refusal-to-modify-fifa-loot-boxes>.

50. See Whitman, *supra* note 45.

51. At the federal level, the United States declared that loot boxes are not gambling. At the state level, however, some states have decided the mechanic is gambling and have enacted legislation accordingly. Compare Whitman, *supra* note 45, with Bailey, *supra* note 24.

52. See Bailey, *supra* note 24.

53. See *id.*

54. *Conmey v. MacFarlane*, 97 Pa. 361, 363 (Pa. 1881) ("A simple contract . . . without consideration, is void, and no action can be maintained upon it."); RESTATEMENT (SECOND) OF CONTRACTS § 71 (AM. LAW INST. 1981). See *MedVet Assoc., Inc. v. Sebring*, 870 N.E.2d 268, 270 (Ohio Misc. 2007); *Roberts v. Gaskins*, 486 S.E.2d 771, 773 (S.C. Ct. App. 1997).

55. Andrew E. Freedman, *What Are Loot Boxes? Gaming's Big New Problem, Explained*, TOM'S GUIDE, <https://www.tomsguide.com/us/what-are-loot-boxes-microtransactions,news-26161.html> (last updated Feb. 27, 2018) ("Loot boxes are digital grab bags. . .").

they already have or an item they do not want.⁵⁶ This lack of consideration makes a loot box comparable to a slot machine.

The second argument, focusing on the requirement to purchase loot boxes, is almost negligible. Individuals are never required to gamble at a casino, but still the industry is regulated.⁵⁷ Video game players are indeed able to enjoy the in-game content without partaking in the loot box mechanic. But the desire to stand out in the virtual world—either aesthetically or through superior performance—often entice players to acquire the in-game currency required to purchase the loot boxes.

Loot boxes are also considered gambling because of the similar psychological effects. A study performed in Australia examined the psychological enticement to gambling.⁵⁸ The study was performed on behalf of Australian legislators to determine the appropriate legal status of video game loot box mechanics.⁵⁹ The study discovered that those who already had a serious gambling problem were more inclined to spend money on loot boxes.⁶⁰ The report also mentioned that the loot box mechanic can serve as a “gateway” to developing a gambling addiction.⁶¹

The very design of the loot box mechanic purposefully persuades players to “buy just one more.”⁶² Some video games, such as Fortnite, are designed to be addictive even without a gambling mechanic.⁶³ In fact, video game addiction is increasing in frequency.⁶⁴ Experts have developed detox methods for overcoming a video game addiction.⁶⁵ Video game addiction has even been considered to be similar to “compulsive gambling.”⁶⁶ The video game user experiences elevated levels of dopamine, which is connected with experiencing something

56. Another interesting comparison to loot boxes is trading card packs. Purchasers are able to purchase a trading card pack and receive cards he or she already has or cards he or she does not want.

57. *See generally* N.J. ADMIN. CODE § 13:69 (2019) (regulating gaming).

58. Prescott, *supra* note 34.

59. *Id.*

60. *Id.*

61. *Id.* (citing the “excitement” to become associated with gambling, which would lead to additional gambling).

62. Alexandra, *supra* note 26.

63. *See* Mel Evans, *Fortnite Is ‘Highly Addictive’ But It’s Parenting That’s the Problem, Claims Expert Who Insists on Hour Limit for Kids*, METRO UK (Mar. 8, 2018), <https://metro.co.uk/2018/03/08/fortnite-highly-addictive-parenting-problem-claims-expert-insists-hour-limit-kids-7371877>.

64. Sherry Rauh, *Detox for Video Game Addiction?*, CBS NEWS (July 3, 2006, 6:35 AM) <https://www.cbsnews.com/news/detox-for-video-game-addiction/>.

65. *Id.*

66. *Id.*

unexpected and positive.⁶⁷ Moreover, the opportunity to enter a new world and temporarily escape from reality also contributes to the development of an addiction.⁶⁸ Parents have also felt the addiction, stating they lost their children to video games.⁶⁹

Now, factor in the loot box mechanic: players are able to try their luck at winning a grand prize in their own fantasy world. The fantasy world now also contains the excitement and psychological effects of gambling. An individual who has to play just one more time to win back their losses demonstrates the gambling addiction.⁷⁰ This parallels the loot box mechanic, which makes the player feel the need to open an additional box to earn a special item and justify any money spent. It is that parallel that is motivating state legislators—and legislators in other countries—to enact laws to prevent children from accessing this sort of mechanic.⁷¹

The loot box situation is additionally dangerous because children are easily impressionable. Children are especially vulnerable to the emotional rush of loot boxes and to the endorsements of popular YouTube vloggers and celebrities who are promoting loot boxes.⁷² Studies show that parents have a significant effect on the development of children.⁷³ When that influence is replaced by loot boxes and celebrities, children have little opportunity to avoid the addiction of gambling. New

67. *Id.*; Phil Newton, *What Is Dopamine?*, PSYCHOL. TODAY (Apr. 26, 2009), <https://www.psychologytoday.com/us/blog/mouse-man/200904/what-is-dopamine/>.

68. Rauh, *supra* note 64 (“[A]n intelligent child who is unpopular at school can ‘become dominant in the game.’”). Reality for children can be much more difficult than fighting a battle online. It was reported that 49% of children in 4th to 12th grades reported being bullied once over a one-month period. Catherine P. Bradshaw et al., *Bullying and Peer Victimization at School: Perpetual Differences Between Students and School Staff*, 36 SCHOOL PSYCHOL. REV. 361, 368 (2007).

69. Petula Dvorak, *The Summer of Pale: How I Lost My Children to Fortnite*, WASH. POST (July 26, 2018), https://www.washingtonpost.com/local/the-summer-of-pale-how-i-lost-my-children-to-fortnite/2018/07/26/ae586d0e-90e9-11e8-b769-e3fff17f0689_story.html?noredirect=on&utm_term=.8f138e16d9e7; Melissa L. Fenton, *What the Heck Is Fortnite, and Why Are My Kids Obsessed With It?*, SCARY MOMMY, <https://www.scarymommy.com/kids-obsessed-with-fortnite/> (last visited Sept. 21, 2018).

70. *Compulsive Gambling Symptoms, Causes and Effects*, PSYCHGUIDES, <https://www.psychguides.com/guides/compulsive-gambling-symptoms-causes-and-effects/> (last visited Sept. 20, 2018) (“If you feel like you need to try just one more time . . . it is highly likely you are suffering from a gambling addiction.”).

71. Alexandra, *supra* note 26 (quoting Hawaiian and New Hampshire senators). MacDonald, *supra* note 20 (providing an anti-loot box quote from the Belgian Minister of Justice).

72. MacDonald, *supra* note 20 (“Mixing games and gambling, especially at a young age, is dangerous for mental health . . .”).

73. Bethel Moges & Kristi Weber, *Parental Influence on the Emotional Development of Children*, VANDERBILT DEVELOPMENTAL PSYCHOL. BLOG (May 7, 2014), <https://my.vanderbilt.edu/developmentalpsychologyblog/2014/05/parental-influence-on-the-emotional-development-of-children/>.

Jersey courts have held that children should not be able to enter casinos.⁷⁴ Casinos in violation of this rule are strictly liable.⁷⁵ Such legislation demonstrates a state's interest in preventing children from gambling exposure.

One example of a celebrity promotion is YouTube celebrity, "Ninja," wanting a loot box in Fortnite.⁷⁶ Ninja creates YouTube videos of himself playing various video games. Famous for his over-the-top behavior, Ninja has over 22 million subscribers on his channel.⁷⁷ This figure does not include any of his videos that are located on other channels.⁷⁸ This also does not take into account his presence on the game streaming website Twitch.⁷⁹ His income of roughly \$500,000 a month demonstrates his influence.⁸⁰

It is important to note that the industry is self-regulating. For example, the Entertainment Software Rating Board (ESRB) was originally created to address video game violence and assign ratings for games.⁸¹ The ESRB itself does not have much authority to regulate the video game industry.⁸² It predominately provides advisories to video game players, such as a "game rating."⁸³ The game ratings range from "E" for everyone to "M" for mature and indicate any controversial elements of the game.⁸⁴

The ESRB now requires labels indicating games with in-game purchases.⁸⁵ The label requirement will apply to games with various

74. *New Jersey v. Boardwalk Regency Corp.*, 548 A.2d 206, 211 (App. Div. 1988); *see also* *Rouso v. Washington*, 239 P.3d 1084, 1091 (Wash. 2010) (recognizing that regulation of gambling is partially motivated by the prevention of underage gambling).

75. *Id.*; *see* N.J. ADMIN. CODE § 5:12-119(a) (2019).

76. Fortnite Records, *Ninja Wants a Ninja Loot Box in Fortnite*, YOUTUBE (May 3, 2018), <https://www.youtube.com/watch?v=YVY0sdfjO7Q>.

77. Ninja, YOUTUBE, <https://www.youtube.com/user/NinjasHyper> (last visited June 28, 2019).

78. Nathan Grayson, *Ninja Takes Two-Day Break, Loses 40,000 Subscribers*, KOTAKU (June 13, 2018, 7:30 PM), <https://kotaku.com/ninja-takes-two-day-break-loses-40-000-subscribers-1826813300>.

79. Ninja, TWITCH, <https://www.twitch.tv/p/about> (last visited May 13, 2019).

80. Joe Colquhoun, *Fortnite Streamer Ninja Makes \$500k per Month*, PC GAMES^N (Mar. 7, 2018), <https://www.pcgamesn.com/fortnite/ninja-streamer-growth> (noting that 50% of the profit comes from Twitch Prime subscriptions). Ninja also earned a spot on the list of *Time's* Top 25 Most Influential People on the internet. *The 25 Most Influential People on the Internet*, TIME, <https://time.com/5324130/most-influential-internet/> (last updated June 30, 2018).

81. Good, *supra* note 22.

82. *Id.*

83. *Id.*

84. *ESRB Ratings*, ENTERTAINMENT SOFTWARE RATING BOARD, <http://www.esrb.org/ratings/> (last visited Oct. 24, 2018).

85. *ESRB Adding Labeling for Loot Boxes, Other 'In-Game Purchases,'* POLYGON, <https://www.polygon.com/2018/2/28/17062424/loot-boxes-esrb-rating-warning-labels-crates>

in-game purchase mechanics including the loot box, season passes, subscriptions, and bonus levels.⁸⁶ Whether or not ESRB took this initiative based on its own desires or from social pressure is unclear.⁸⁷

Apple is taking its own approach by requiring that publishers disclose the statistics behind loot boxes.⁸⁸ Specifically, any application that provides “randomized virtual items for purchase must disclose the odds of receiving each type of item”⁸⁹ Apple, the first major company to require publisher disclosures, has already applied this requirement to major games such as *Heartstone*.⁹⁰ It is likely that this rule will also apply to the iOS version of *Fortnite*.

The reception of the labeling requirement is divided. Some believe the actions are not enough.⁹¹ By grouping the loot box mechanic with general in-game purchases, this approach is not giving parents and individuals enough information to act accordingly.⁹² One study demonstrated that even if parents knew what a loot box was, they did not fully understand what the loot box entailed.⁹³ Part of the international effort is to ensure parents understand the risk of loot boxes as well as unlicensed third party attempts to sell loot boxes to children.⁹⁴ Authorities are attempting to crack down on the issue through parental education and involvement.⁹⁵ Information will allow parents to make the decision regarding the child’s exposure to loot box mechanics in video games, ranging from unrestricted access to absolute prohibition.

On the other side of the argument, a developing campaign contends the parental controls available in the video game console are sufficient to handle the issue.⁹⁶ The actual video game consoles have expanded

(last updated Feb. 27, 2018). *But see* Elliot O’Day, *21st Century Casinos*, 19 TEX. TECH. ADMIN. L.J. 365, 366 n.6 (2018) (stating that the ESRB equates loot boxes to collecting baseball cards).

86. Owen S. Good, *The ESRB’s New Warning Seems to Hide Loot Boxes in Plain Sight*, POLYGON (Mar. 3, 2018, 3:40 PM), <https://www.polygon.com/2018/3/3/17075936/esrb-warning-label-loot-crates-in-game-purchases-battlefront-2>.

87. *See* Alexandra, *supra* note 26 (noting that a New Hampshire senator called for ESRB action).

88. *Id.*

89. Chaim Gartenberg, *Apple Now Requires Games with Loot Boxes to Disclose Odds*, VERGE (Dec. 21, 2017, 11:05 AM), <https://www.theverge.com/2017/12/21/16805674/apple-loot-box-app-store-games-odds-probability-disclosure>.

90. *Id.*

91. Good, *supra* note 86.

92. *Id.*

93. Good, *supra* note 22.

94. Wade, *supra* note 40.

95. Connor Hume, *Gambling Regulators Sharpen Focus on Loot Boxes & Social Gaming*, LEXOLOGY (Sept. 24, 2018), <https://www.lexology.com/library/detail.aspx?g=048ebd1a-8f2a-47c0-be00-d63f3a935ec6>.

96. Good, *supra* note 22.

parental controls that prevent children from purchasing in-game content with real world currency.⁹⁷ With the lack of regulation, the ESRB recommends that parents take advantage of these controls.⁹⁸ Unfortunately, a parent is not always aware of the parental controls. Additionally, some “technologically savvy” children are able to disable parental controls. Thus, such an approach is not a viable solution.

One possible action some video game publishers have already taken is to disclose the “drop rates” of their loot boxes.⁹⁹ Some companies, possibly hoping they can get in front of any legislation and win the admiration of their customers, provide players statistics of the likelihood of winning a certain item.¹⁰⁰ The disclosure of the loot box system may also allow publishers to keep their products in foreign markets.¹⁰¹ For example, a regulation in China prohibits the sale of any game that does not provide the probability of obtaining an item from a loot box.¹⁰² As noted above, Apple has done something similar, and Google has as well.¹⁰³

The loot box mechanic is not going away. Video game developers and publishers have been improving video games overall, but they have not raised prices despite the sharp increase in the cost of developing video games, which is now roughly ten times more expensive than before.¹⁰⁴ Loot boxes are one approach that these companies have taken to raise the revenue. For example, Activision Blizzard made approximately half of its \$7 billion revenue from microtransactions in general.¹⁰⁵ Moreover,

97. *XboxOne*, ENTERTAINMENT SOFTWARE RATING BOARD, <http://www.esrb.org/about/parentalcontrol-xbox.aspx> (last visited Sept. 19, 2018). The ESRB also provides controls for other consoles. *ESRB Parent Resources Center*, ENT. SOFTWARE RATING BOARD, <http://www.esrb.org/about/settingcontrols.aspx> (last visited Sept. 19, 2018).

98. See Good, *supra* note 22.

99. Alexandra, *supra* note 26.

100. *Id.*; Nathan Grayson, *Blizzard Reveals Overwatch Loot Box Odds in China*, KOTAKU (May 5, 2017, 11:57 AM), <https://kotaku.com/blizzard-reveals-overwatch-loot-box-odds-in-china-1794956138>; Julia Lee, *Riot Games Reveals League of Legends Loot Box Rates*, RIFT HERALD (Feb. 22, 2018, 2:12 PM), <https://www.riftherald.com/lol-gameplay/2018/2/22/17041132/league-of-legends-loot-box-rates-hextech-crafting-riot-games>.

101. Alexandra, *supra* note 26.

102. Nordmark, *supra* note 37.

103. Gartenberg, *supra* note 89; Ethan Gach, *Google Now Requires App Makers to Disclose Loot Box Odds*, KOTAKU (May 30, 2019, 6:10 PM), <https://kotaku.com/google-now-requires-app-makers-to-disclose-loot-box-odd-1835134642>.

104. MacDonald, *supra* note 20 (noting that games have stayed at the same \$50–\$60 price range over fifteen years).

105. Rob Thubron, *Over Half of Activision Blizzard’s \$7.16 Billion Yearly Revenue Came from Microtransactions*, TECHSPOT (Feb. 12, 2018), <https://www.techspot.com/news/73230-over-half-activision-blizzard-716-billion-yearly-revenue.html> (“\$4 billion of that amount came from ‘in-game net bookings,’ which covers loot boxes, sales of DLC, and in-app purchases.”).

some developers implement loot box mechanics to keep pace with their competitors.¹⁰⁶

Aside from the likeness to gambling, the general gaming community dislikes the loot box mechanic. Publishers have experienced severe backlash from their customers when the loot box was too central to the game. The most recent example occurred in EA Star Wars Battlefront 2.¹⁰⁷ Battlefront's progression system seemed to require advantages obtained either through a direct purchase or through the purchase of loot boxes. In-game purchases let players skip ahead to the access of major characters of the Star Wars universe as well as to purchase character improvements.¹⁰⁸ In other words, the purchase of loot boxes allowed players to skip earning in-game currency through the traditional method of playing the game, dedicating time and effort, and competing against other players. The frustration was heard on social media and online forums such as Reddit.¹⁰⁹ The gaming community backlash and criticism eventually led EA to remove the mechanic.¹¹⁰ The removal was even accompanied by an apology from an EA executive.¹¹¹

While the long-term social effects are still unclear at this point, the increased exposure to sports betting may normalize gambling. Loot box mechanics, whether legally classified as gambling or not, have the same psychological effects as gambling. If gambling is more socially acceptable, the likelihood of successful loot box mechanic regulation might decrease. Conversely, the possibility of exposing children to loot box mechanics and the psychological effects of gambling increases. Even worse, parents will have no idea what their children are being exposed to.

III. CONCLUSION

Loot boxes are a new development, along with the rise of in-game purchases in general.¹¹² Since these mechanics are so new, legislators and the general public are unaware of what they are or how to treat them. General in-game purchases, while aggravating to some, do not involve

106. *Id.*

107. Tae Kim, *EA Vows to Never Offer Paid 'Loot Boxes' in Its Controversial 'Star Wars Battlefront II' Game*, CNBC (Mar. 16, 2018, 1:46 PM), <https://www.cnn.com/2018/03/16/ea-vows-to-never-offer-paid-loot-boxes-in-its-controversial-star-wars-battlefront-ii-game.html>.

108. Ben Gilbert, *The Latest Major 'Star Wars' Game Finally Dropped Its Most Controversial Aspect—But It May Be Too Late*, BUS. INSIDER (Mar. 16, 2018, 10:40 AM), <https://www.businessinsider.com/star-wars-battlefront-2-drops-loot-boxes-2018-3>.

109. Kim, *supra* note 107.

110. *Id.*

111. Andrew Webster, *EA Says It's Learned from Star Wars Battlefront Controversy, Vows to 'Be Better,'* VERGE (Apr. 13, 2018, 8:59 AM), <https://www.theverge.com/2018/4/13/17230874/ea-star-wars-battlefront-2-loot-box-patrick-soderlund-interview>.

112. Activision Blizzard reported billions in revenue in each quarter. Nordmark, *supra* note 37.

much danger other than a higher credit card bill. However, loot boxes are different because they mimic gambling and should be regulated as such.

The world has been slow to respond. Loot boxes have been active for several years now, but very few countries have taken action to address the mechanic. Several states have started to address the issue, but most legislation that has been proposed has yet to be adopted or to take effect. Meanwhile, the effects of loot boxes, in terms of addiction, are being documented. Video game developers mainly target children despite their inability to understand the mental effects of loot box mechanics. Despite a nation-wide acceptance of the prohibition on underage gambling, it seems as if there is an apathy to virtual gambling with real money. Perhaps it is the virtual separation that justifies loot boxes? Users are not directly gambling, but gambling through their virtual identity with their real-world money. Regardless of how they are viewed, loot boxes should be statutorily regulated. Any applicable laws would not regulate the general game, just the ability to access the loot box mechanic. Additionally, parents should be educated on what is going on in their children's lives.

A NEW AGE OF AUTHENTICATION

*Abraham Oxner**

INTRODUCTION	229
I. THE ISSUE.....	230
II. THE EVOLUTION	235
III. THE IMPLEMENTATION	239
CONCLUSION.....	245

INTRODUCTION

The American justice system is predicated upon proving the validity of your argument to a trier of fact. It is apparent that proving your argument requires evidence. This is the challenge that all trial attorneys face. However, before evidence can be presented to a fact finder, it must be admitted.¹

In general, the admission of evidence is a long and complex process. There are several hurdles in place that an attorney must overcome before a piece of evidence is ever placed in front of a jury. A full-length discussion of those hurdles is beyond the scope of this Note. What is important to note, however, is that all evidence must be authenticated.² Authentication, in many cases, forces the entering party to prove the evidence is what they claim it to be.³ This evidentiary hurdle is so obvious that it is often overlooked. However, in scholarly literature or legal jurisprudence, this seemingly simple requirement is a quagmire when applied to purely digital evidence or electronically stored information (ESI).

The timeliness of this discussion is influenced by the Amendment to the Federal Rules of Evidence on December 1, 2017.⁴ One of those amendments added two ESI-specific provisions to Rule 902 to allow more types of evidence to be “self-authenticating.”⁵ This Note will examine how the legal system has navigated the newest hurdle of

* J.D., University of Florida Levin College of Law (2019); B.A., University of South Florida (2011).

1. *See* FED. R. EVID. 402.

2. *See id.* 401(a), 901(a).

3. *Id.* 901(a).

4. *See* Carl A. Aveni, *New Federal Evidence Rule Changes Reflect Modern World*, LITIG. NEWS, Spring 2018, at 10.

5. *Id.*; FED. R. EVID. 902(13), (14).

authenticating ESI and to determine what other solutions may lay on the horizon.

Section I will give a historical background as to how courts have previously handled the growth of ESI and the unique challenges it presents. Section II will outline the most recent adaptation directly related to authentication and explain how the changes were meant to work. Finally, Section III will assess the implementation of the amendments, identify remaining issues, and suggest solutions.

I. THE ISSUE

Historically, the amount of evidence produced and used in court had been organically capped at a manageable amount due to the physical limitations of paper-documents, both in storage space and transmission.⁶ Today, however, the world communicates digitally. The failure to adapt to this considerable shift in the character of evidence was a major critique of the Federal Rules of Evidence.⁷

A digital wave of data swept the globe and had a profound impact on how courts had to handle the use and storage of this potential evidence. In 1999, a University of California study found that 93% of information was created digitally in that year.⁸ In 2000, the approximate cost to store 1GB of data electronically was \$14.⁹ That price plummeted to 75¢ by 2005.¹⁰ In 2015, the cost was around 3¢.¹¹ With such stunning reduction in storage costs, the presumption would be that the promulgation of ESI has made litigation cheaper. Yet, the cost of preserving this information grew exponentially, and by 2014, larger companies reported spending upwards of \$40 million on simply maintaining this data.¹²

The reason for this inverse increase in cost relates to the first and most prominent challenge in dealing with ESI: volume.¹³ Companies today deal in terabytes of data as the majority of companies' stored information

6. See Kenneth J. Withers et al., *Panel One: Technical Aspects of Document Production and E-Discovery*, 73 *FORDHAM L. REV.* 23, 25 (2004).

7. AM. COLL. OF TRIAL LAWYERS TASK FORCE ON DISCOVERY & INST. FOR THE ADVANCEMENT OF THE AM. LEGAL SYS., FINAL REPORT ON THE JOINT PROJECT OF THE AMERICAN COLLEGE OF TRIAL LAWYERS TASK FORCE ON DISCOVERY AND CIVIL JUSTICE AND IAALS 2 (2009), https://iaals.du.edu/sites/default/files/documents/publications/actl-iaals_final_report_rev_8-4-10.pdf.

8. MICHAEL R. ARKFELD, *ARKFELD ON ELECTRONIC DISCOVERY AND EVIDENCE* § 1.1 (4th ed. Supp. 2019).

9. Andrew Bartholomew, *Rethinking "Cheap" Data Storage*, *EXTERRO* (June 10, 2015), <https://www.exterro.com/blog/rethinking-cheap-data-storage/>.

10. *Id.*

11. *Id.*

12. *Id.*

13. See *id.* and accompanying text.

is electronic.¹⁴ Additional sources, such as Facebook and Twitter posts or cell phone text messages, add to the volume of discovery. UC Berkeley's School of Information Management and Systems reported five exabytes of data were created globally in 2002.¹⁵ By 2006, that number grew to 161 exabytes.¹⁶ Research shows that approximately 124.5 billion business emails were sent each day in 2018, with that number expected to grow by 3% in 2019.¹⁷ It is society's overwhelming dependence upon technology—especially in business—which has exacerbated the growth of ESI each year and compounded the difficulties faced in authenticating such data.

A second feature of ESI that poses particular difficulty for authentication is its complexity. Traditionally, the authentication of paper evidence was a matter of reading what was written on the page. The Rules of Evidence were devised to determine the reliability and authenticity of this type of information.¹⁸ However, ESI is deceptively detailed as it contains layers of embedded metadata, which can sometimes be its most valuable asset.¹⁹

Third, ESI is subject to, and almost completely dependent upon, the devices within which it is stored. For example, emails and text messages are not stored in printed form but through a systems inbox. This creates a subset of problems for all phases of admissibility because it creates more chains of custody as the data can be manipulated, deleted, or lost due to imprecise system storage or user error.²⁰ ESI is frequently destroyed inadvertently by being deleted or overwritten as a routine, good faith business practice.²¹ Ironically, the opposite problem of being able to locate or recreate deliberately deleted data can also give rise to

14. Damian Vargas, *Electronic Discovery: 2006 Amendments to the Federal Rules of Civil Procedure*, 34 RUTGERS COMPUTER & TECH. L.J. 396, 398 (2008).

15. PETER LYMAN & HAL R. VARIAN, U.C. BERKELEY, SCH. INFO. MGMT. SYS., HOW MUCH INFORMATION? (2003), <http://groups.ischool.berkeley.edu/archive/how-much-info-2003/execsum.htm>.

16. Geoff Duncan, *Study: 161 Exabytes of Digital Data in 2006*, DIGITAL TRENDS (Mar. 6, 2007, 3:00 AM), <https://www.digitaltrends.com/computing/study-161-exabytes-of-digital-data-in-2006/>.

17. Andrea Robbins, *The Shocking Truth About How Many Emails Are Sent*, CAMPAIGN MONITOR (Mar. 19, 2018), <https://www.campaignmonitor.com/blog/email-marketing/2018/03/shocking-truth-about-how-many-emails-sent/>.

18. FED. R. EVID. 901(a).

19. See Withers et al., *supra* note 6, at 24.

20. Adam Stone, *How to Ensure Digital Evidence Stands Up in Court*, GEN. DYNAMICS INFO. TECH. (Sept. 17, 2015), <https://www.govtechworks.com/chain-of-custody-how-to-ensure-digital-evidence-stands-up-in-court/>.

21. BARBARA J. ROTHSTEIN ET. AL., FED. JUDICIAL CTR., MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 19–20 (2007).

complications for authentication.²² Additionally, because ESI does not stand alone, it requires potentially expensive or inaccessible computing systems to present all the information in a way that is understandable and reasonable for judges and juries.

These features of ESI create complications that implicate more than just the Evidence Code. Though authentication is the current topic of discussion, the Federal Rules of Civil Procedure were amended when ESI first burst onto the legal landscape.²³ The primary concern was the confusion and cost involved when handling large quantities of ESI in the discovery phase.²⁴ How did the Federal Rules of Civil Procedure regarding discovery handle unduly burdensome obligations of businesses and individuals to store and preserve ESI and the accompanying hefty sanctions when they erred? The response came in 2006 with an amendment to the Federal Rules of Civil Procedure, which recognized ESI as distinct from paper-based document discovery, and created methods of reducing discovery costs and sanctions.²⁵ The background and resolution of the early 2000s ESI challenges for discovery provide a useful comparison to the authentication challenges and subsequent 2017 amendments to the Federal Rules of Evidence that address them.

The groundbreaking series of opinions in 2003 from *Zubulake v. UBS Warburg LLC* demonstrated the need for the 2006 amendments to the Federal Rules of Civil Procedure.²⁶ Briefly, the *Zubulake* case dealt with a discrimination suit against a former employer in which the plaintiff requested hundreds of email records that the defendant only partially complied with.²⁷ The attorney for the defense mistakenly believed that the emails in question had been “archived” when, in reality, the employee who wrote the emails had simply saved them to a folder where they were later deleted.²⁸ The defendant then claimed that the cost and volume of the documents had created an undue burden as many were inaccessible or deleted, and the cost of finding and reviewing the backups was over \$300,000.²⁹ Ultimately, the court modified the existing “inaccessibility”

22. *See id.* at 10.

23. Samantha V. Ettari, *Sanctions Under Amended FRCP 37(e): One Year In*, PRAC. L., Dec. 2016/Jan. 2017, at 14, <https://www.kramerlevin.com/images/content/1/7/v4/1748/Sanctions-Under-Amended-FRCP-37-e-One-Year-In-Sam-Ettari.pdf>.

24. *See* Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 NW. J. TECH. & INTELL. PROP. 171, 181–183 (2006).

25. *Id.* at 172–73.

26. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003).

27. *Id.* at 312.

28. *Id.* at 311–12.

29. *Id.* at 313.

test and created a new seven-factor test for e-discovery disputes.³⁰ It then found that many of the undisclosed emails were not inaccessible and instructed the jury that they were permitted to assume the missing emails would not have favored the defendant.³¹ The court also imposed monetary sanctions on the defendant and, in combination with the damages, the plaintiff won almost \$30 million.³² This result epitomized the confusion on the applicable standard for ESI discovery. Thus, it is clear why the amendments to the Federal Rules of Civil Procedure—arriving one year after *Zubulake*—focused on “parties’ legitimate worries about sanctions, production costs, and the burdens and expenses of privilege review.”³³

The 2006 amendments created ESI as an independent form of discovery evidence.³⁴ They further developed new rules of procedure to govern ESI discovery, including an exception for ESI if the court deems the requested ESI to be not reasonably accessible to the producing party.³⁵ The remaining changes attempted to clarify the obligations of companies in preserving and later producing requested ESI.³⁶ The amendments created “safe harbor” periods for ESI that was destroyed or lost in the regular course of business by a data storage system.³⁷

The early 2006 amendments to the Federal Rules of Civil Procedure were an acknowledgement by the Advisory Committee of the expanding use of ESI. Courts attempted to work around the outdated rules and create common law that could process electronic evidence. Instead, confusion abounded, and it took formal amendments to standardize and stabilize the courts. Today, the admissibility of ESI is similarly hindered by the antiquity of the Evidence Code. In the case law that follows, attempts are made to create common law to authenticate ESI for admissibility, and these attempts are similar to those discussed above relating to discovery.

One of the earlier examples of courts fitting ESI into the boundaries of the Rules of Evidence is *In re Vee Vinhnee*.³⁸ In the opinion, the court stated that “[a]uthenticating a paperless electronic record, in principle,

30. *Id.* at 321–24.

31. *Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422, 439–40 (S.D.N.Y. 2004).

32. Eduardo Porter, *UBS Ordered to Pay \$29 Million in Sex Bias Lawsuit*, N.Y. TIMES (Apr. 7, 2005), <https://www.nytimes.com/2005/04/07/business/ubs-ordered-to-pay-29-million-in-sex-bias-lawsuit.html>.

33. Rachel Hytken, *Electronic Discovery: To What Extent Do the 2006 Amendments Satisfy Their Purpose?*, 12 LEWIS & CLARK L. REV. 875, 880 (2008).

34. FED. R. CIV. P. 26(b)(2)(B).

35. *Id.*

36. *See id.* 34(b) advisory committee’s note to 2006 amendment; *id.* 37(f) advisory committee’s note to 2006 amendment.

37. *Id.* 37(e) (2006) (repealed 2015).

38. 336 B.R. 437 (B.A.P. 9th Cir. 2005).

poses the same issue as for a paper record”³⁹ However, the court then went into great detail as to how a proper foundation may be laid to authenticate ESI using principles from Rules 901 and 902.⁴⁰ For a point of reference, the court looked to Professor Imwinkelried’s writings on digital paperless business records as scientific evidence and lists eleven steps that are generally appropriate to lay foundation.⁴¹ Many of these steps, however, are deceptively simple, such as a showing that “the computer” from which the ESI is pulled “is reliable.”⁴² Thus, the *In re Vee Vinhnee* court minimized the unique challenge of authentication rather than relying on a workable, scientific approach for future guidance.⁴³ This analysis shows the striking incongruity between a perceived simplicity of handling ESI with the current Rules and the attempt at creating a new scientific methodology to accomplish this goal.

The landmark case of *Lorraine v. Markel American Insurance Co.* reflects the continued entanglement of the Rules of Evidence when applied to ESI.⁴⁴ The key issue dealt with the language of an arbitration agreement to settle an insurance claim on a destroyed yacht.⁴⁵ The judge dismissed both the plaintiff’s and defendant’s motions for summary judgment, stating that neither party had entered enough evidence.⁴⁶ In summary judgment, only evidence that would be admissible in court can be relied upon, but neither party offered anything to support the authentication of the emails.⁴⁷ *Lorraine* was a realization of the extra steps required for authentication when dealing with ESI.⁴⁸ The failure of either side to fit ESI into the Rules of Evidence as they existed at the time—particularly Rule 901—was a major contributor to the ultimate inadmissibility of the parties’ evidence.⁴⁹

As ESI has developed, the rules governing it have been slow to evolve alongside it. Before discussing the 2017 amendments to the Rules of Evidence, it will be useful to give context for the previously detailed irregularities of ESI by noting the Rules of Evidence regarding authentication as they existed prior to the 2017 amendments. Following this, the 2017 additions and any potential implications they may have concerning Rule 902 will be analyzed.

39. *Id.* at 444.

40. *Id.* at 446–47.

41. *Id.*

42. *See id.* at 446.

43. *Id.* at 444–45

44. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007).

45. *Id.* at 535.

46. *Id.* at 537.

47. *Id.* at 535.

48. *See id.* at 542–43.

49. *See id.* at 541–42.

II. THE EVOLUTION

As with anything involving the Federal Rules of Evidence, the authentication process is a multi-layered interplay between several different rules. To best understand the process, it will be helpful to start broadly with the language of Rule 104. Rule 104(a) states: “The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.”⁵⁰ Generally, Rule 104(a) means that a judge makes the first determination of admissibility based on the offered support of authenticity, and the question goes to a jury only if it becomes reasonable to believe that the condition has not been met.⁵¹

The difficulty begins with Rule 104(b), which reads: “When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.”⁵² This has been interpreted to mean that when the fact used to prove authenticity under Rule 104(a) is disputed, extrinsic evidence must be brought in.⁵³ This may sound like a niche scenario, but this situation occurs much more frequently when dealing with ESI. For example, an email or text message can fall under 104(b) if the authorship is asserted by one party but denied by the other.⁵⁴ No evidence of handwriting analysis or possession of a physical copy is available. In this situation, a judge may allow the evidence before the jury and hear testimony as to its authenticity while instructing the jury to disregard it if they are not convinced.⁵⁵

More commonly, judges may require additional authenticity support for ESI evidence even if it is not a Rule 104(b) fact issue due to the skepticism of this form of information.⁵⁶ It is important to note that this form of proving authentication is distinct from that of a Rule 104(b) factual dispute. In the latter situation, the trial judge is still the decision-maker.⁵⁷ However, when the judge has allowed the evidence before a jury to hear testimony as to its authenticity, the party attempting

50. FED. R. EVID. 104(a).

51. *Id.* 104 advisory committee’s notes to 1972 proposed rule.

52. *Id.* 104(b).

53. *See id.* 104 advisory committee’s notes to 1972 proposed rule.

54. *See id.*

55. *See* Paul W. Grimm et al., *Authenticating Digital Evidence*, 69 BAYLOR L. REV. 1, 5 (2017).

56. *See id.* at 6.

57. *See* Symposium, *The Challenges of Electronic Evidence*, 83 FORDHAM L. REV. 1163, 1175–76 (2014).

to enter the exhibit must turn to Rule 901.⁵⁸ Rule 901(a) states: “To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.”⁵⁹ Rule 901(b) offers a list of ways in which a party may authenticate its evidence to the judge.⁶⁰ Which of the listed methods is most appropriate depends on what type of evidence the party is attempting to admit.⁶¹ Rule 902 also plays a role here, as it provides a list of things that are considered “self-authenticating.”⁶² This will be explored later due to its importance to the 2017 amendment.

In relation to the differences in ESI and traditional evidence discussed in Part I, many digitally created documents fall under Rule 901.⁶³ It is uncommon that a piece of ESI would be deemed inadmissible by a judge because the threshold for authenticity is low.⁶⁴ However, costs can become very burdensome when there is a high volume of ESI and the authentication is at issue.⁶⁵ ESI, like social media postings or chat room conversations, are often created through anonymous usernames or third parties.⁶⁶ Emails are at a notoriously high risk of being hacked and may require testimony towards authorship.⁶⁷ Similarly, text messages require testimony of authorship and are easily deleted.⁶⁸ The number of witnesses required to prove a threshold level of authenticity has become increasingly cumbersome and expensive as the world becomes increasingly more digitized.

When the Advisory Committee on Evidence met in 2017, there was once again an emphasis on reducing the costs associated with handling ESI.⁶⁹ Primarily, this meant reducing the number of witness testimonies required.⁷⁰ As previously mentioned, Rule 902 also governs the authentication of evidence.⁷¹ Rule 902 lists several different types and methods of self-authenticating evidence, which require no extrinsic evidence, such as testimony, to support them.⁷² Before the 2017

58. *See id.* at 1173.

59. FED. R. EVID. 901(a).

60. *Id.* 901(b).

61. *See id.*

62. *Id.* 902.

63. *Id.* 901(a).

64. Grimm et al., *supra* note 55, at 11–12.

65. *See id.* at 12.

66. *Id.* at 22.

67. *Id.* at 12–13.

68. *Id.* at 19.

69. *Id.* at 38.

70. *Id.*

71. FED. R. EVID. 902.

72. *Id.*

amendments, Rule 902 had only limited use for ESI. For example, Rule 902(11) often admitted emails as regularly conducted business activity, similar to the business record exception to hearsay.⁷³

However, the Rule 902 options did not neatly identify any types of ESI and frequently led to unworkable results. In *United States v. Browne*, incriminating messages were sent on Facebook and the prosecutor sought to admit them.⁷⁴ In order to authenticate these messages, the prosecutor brought in a certification of a records custodian from Facebook.⁷⁵ The custodian testified to the fact that storing Facebook messages was a regularly conducted activity as allowed in Rule 902(11).⁷⁶ The court held that this testimony made no showing that the defendant was actually the one who authored the messages as the custodian had no personal knowledge.⁷⁷ The court noted that this form of testimony would authenticate the metadata in the messages and the timestamp of when they were sent and received, but not the content of the messages.⁷⁸

Similarly, some of the provisions of Rule 902 have had their language stretched to adapt to and include more reliable forms of ESI.⁷⁹ This had been the pre-2017 amendment trajectory to ease ESI litigation expenses without having to change or alter the Federal Rules of Evidence. For example, in *Williams v. Long*, the plaintiffs submitted printed webpages from a government website as evidence and offered no support for their authentication.⁸⁰ When determining whether to admit the webpages, the court turned to Rule 902(5) and summarized that Rule as allowing “extrinsic evidence of authenticity as a condition precedent to the admissibility of evidence is not required if the evidence is a book, pamphlet, or other publication purporting to be issued by a public authority” to be self-authenticating.⁸¹ The court latched on to the words “public authority” and “other publication,”⁸² interpreting these phrases to mean that “if information is published on a website by a public authority and that information is obtained through the FOIA (or, as in this case, an equivalent state act), then that printed information would be self-authenticating under Rule 902(5).⁸³” Thus, websites from legitimate

73. Kevin F. Brady et al., *The Sedona Conference Commentary on ESI Evidence & Admissibility*, 9 SEDONA CONF. J. 217, 220–21 (2008).

74. *United States v. Browne*, 834 F.3d 403, 405–06 (3d Cir. 2016).

75. *Id.* at 408.

76. *Id.*

77. *Id.* at 410.

78. *Id.* at 411.

79. See Grimm et al., *supra* note 55, at 11–33.

80. *Williams v. Long*, 585 F. Supp. 2d 679, 682 (D. Md. 2008).

81. *Id.* at 686.

82. *Id.*

83. *Id.* at 690.

government agencies have traditionally been found to be self-authenticating under Rule 902(5).⁸⁴

Similarly, courts have interpreted Rule 902(6) to allow self-authentication of online newspaper articles.⁸⁵ Rule 902(6) allows “[p]rinted material purporting to be a newspaper or periodical.”⁸⁶ However, Rule 101(b)(6) permits any mention of printed materials within the Rules to also mean and relate to comparable information in electronic form.⁸⁷ Thus, there is no requirement that the online newspaper have ever been printed.⁸⁸

These complex solutions to fit ESI into the Rules of Evidence serve as a backdrop for the 2017 amendments, which made multiple additions to the Federal Rules of Evidence.⁸⁹ However, this Note focuses on the addition of two new subsections of Rule 902, which deal directly with self-authenticating ESI. The new additions read as follows:

(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).⁹⁰

In their simplest form, these additions were made to alleviate much of the interpretive tap-dancing described above.⁹¹ While very little is ever

84. *See id.*; FED. R. EVID. 902(5).

85. *See, e.g.,* White v. City of Birmingham, 96 F. Supp. 3d 1260, 1274 (N.D. Ala. 2015) (admitting newspaper articles from the *Huntsville Times* website into evidence as self-authenticating); *see also* PAUL W. GRIMM ET AL., BEST PRACTICES FOR AUTHENTICATING DIGITAL EVIDENCE 17 (2016).

86. FED. R. EVID. 902(6).

87. *Id.* 101(b)(6).

88. GRIMM ET AL., *supra* note 85, at 17.

89. Carey Busen, *It's the End of Authentication (of ESI) as We Know It*, DISCOVERY ADVOCATE (Nov. 29, 2017), <https://www.discoveryadvocate.com/2017/11/29/its-the-end-of-authentication-of-esi-as-we-know-it/>. In addition to changes to Rule 902, the Amendment also changed portions of the hearsay exception for ancient documents under Rule 803. *Id.*

90. FED. R. EVID. 902(13)–(14).

91. *See supra* Part II.

easy in the Rules of Evidence, the understanding was that, at this point in technological usage, not all ESI is created equal. The allowance of certain more obvious or credible ESI to fit into Rule 902 provisions, such as those discussed above, are an acknowledgment of that fact.

The largest effect these amendments were meant to accomplish relates back to the 2006 amendments. Previously, the 2006 amendments sought to shift the burden of e-discovery costs and ESI litigation back to the requesting party.⁹² In a similar fashion, the 2017 amendments have shifted the burden of authentication back to the party opposing the admission.⁹³ Traditionally, the party seeking to admit ESI had the burden of producing testimony to show authenticity; however, this was considered inefficient.⁹⁴ Often, “the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary because the adversary either stipulates to authenticity before the witness is called or fails to challenge the authentication testimony once it is presented.”⁹⁵ Now, with the mechanisms discussed below, most types of ESI can be more easily authenticated prior to trial and the party opposing it may object if they can show the ESI is not authentic. It is also important to note that the processes used for self-authentication in Rules 902(13) and (14) only work towards certifying authenticity; the evidence is still subject to all other appropriate objections.⁹⁶

This discussion has provided a look at the Rules of Evidence related to ESI, an explanation of how they operate, and early attempts to make ESI conform to them. This discussion demonstrated the necessity of the two added provisions to Rule 902 presented and analyzed above. Part III will focus on projecting how these new Rules will work with the old ones and suggest implementation strategies.

III. THE IMPLEMENTATION

The primary mechanism to the new provisions of Rule 902 is a certificate of authenticity that complies with the three certification requirements of Rule 902 under sections (11) and (12)⁹⁷: “First, the record was made at or near the time by, or from information transmitted by, someone with knowledge. Second, the record was kept in the course of a

92. Bradley T. Tennis, Comment, *Cost-Shifting in Electronic Discovery*, 119 YALE L.J. 1113, 1113–14 (2010).

93. See Paul W. Grimm, *Recent Changes to Federal Rules of Evidence: Will They Make It Easier to Authenticate ESI?*, 19 SEDONA CONF. J. 707, 709 (2018).

94. See *id.*

95. *Id.* at 715.

96. Ramona L. Lampley, *Something Old and Something New: Exploring the Recent Amendments to the Federal Rules of Evidence*, 57 WASHBURN L.J. 519, 528 (2018).

97. FED. R. EVID. 902(13)–(14).

regularly conducted activity of a business, organization, occupation, or calling. Third, making the record was a regular practice of that activity.”⁹⁸ However, due to the nature of ESI, the affiant must additionally certify aspects of the electronic storage and transmission processes involved in obtaining the ESI to meet the chain of custody requirements under Federal Rules of Evidence 401 and 901.⁹⁹ This certificate does not alleviate any of the actual requirements to show authenticity—it merely allows parties to prove authenticity before any hearings and without the need to bring in witnesses.¹⁰⁰ A more detailed discussion of what types of information should be included in the certification of ESI under the new Rules is provided below.

Rule 902(13) deals more specifically with the certification of the electronic process or system that stores ESI.¹⁰¹ The proponent of the evidence must have a qualified person certify that the system is reliable and can accurately store the information.¹⁰² Generally, the certificate should describe the system that generated the ESI, the process used to collect and preserve the data within the system that eventually produced the ESI, and the method used to take the ESI from the system to present it for evidence.¹⁰³

Rule 902(14) uses a similar method for proving authenticity but for a different purpose. The focus of Rule 902(14) is to authenticate ESI that is a copy of a paperless digital information source.¹⁰⁴ One of the most important aspects to understanding how anyone can verify a digital copy of digital information is through the use of “hash values.”¹⁰⁵ These hashes serve as digital fingerprints: when a document matches the hash value of its proposed source, it is an exact duplicate.¹⁰⁶ Thus, hash values should be included in the certification affidavit along with a description of the recording time and date, the method used to make the copy, and any software used.¹⁰⁷ If a qualified person verifies this information under oath, a judge can properly assume that the ESI is authentic without the

98. Edward T. Kang et al., *Self-Authentication of ESI Under Federal Rule of Evidence 902*, LEGAL INTELLIGENCER (June 21, 2018), <https://www.law.com/thelegalintelligencer/2018/06/21/self-authentication-of-esi-under-federal-rule-of-evidence-902/>.

99. *Id.*

100. See Carl Aveni, *New Federal Evidence Rule Changes Reflect Modern World*, LITIG. NEWS, Spring 2018, at 10.

101. FED. R. EVID. 902(13).

102. *Id.*

103. Grimm, *supra* note 93, at 720–21.

104. FED. R. EVID. 902(14).

105. See *id.* 902(14) advisory committee’s note to 2017 amendment; Dennis Martin, *Demystifying Hash Searches*, 70 STAN. L. REV. 691, 700 (2018).

106. Martin, *supra* note 105, at 695, 699.

107. See Kang et al., *supra* note 98.

need for witness testimony. While these steps sound simple, the practice of preserving and collecting this information is complicated and easily ruined if not handled properly.

Furthermore, under Rules 902(13) and (14), the offering party must meet Rule 902(11) requirements for giving notice to opposing counsel of their intent to offer ESI at trial.¹⁰⁸ The opposing counsel may choose not to challenge the certification, thus eliminating the need for the qualified person who wrote the affidavit to be brought to court and questioned. However, there is still the opportunity to challenge authenticity or the described system.¹⁰⁹ If the certificate is challenged, the qualified person will be required to testify at trial and is subject to cross-examination as a witness.¹¹⁰ Thus, many, if not all, of the original hurdles for authenticating ESI still exist, but the work can be done in a more efficient and inexpensive way.

These amendments should streamline the authentication of ESI, and their implementation can be illustrated using two separate examples. In the first example, the cellphone of a criminal defendant is seized and properly searched, resulting in the recovery of incriminating text messages. Prior to the amendments, the prosecutor would have to bring in a forensic technician to testify as to the way cellphones track and store messages with timestamps and metadata.¹¹¹ With the newly added Rule 902(13), the court should allow the forensic technician to provide the same information in an affidavit certifying the authenticity.¹¹²

Similarly, in the second example, if a forensic technician instead made a copy of the cellphone's text message logs, Rule 902(14) could be implemented.¹¹³ Again, prior to these amendments, the technician would have to testify as to how the copies are authentic duplicates.¹¹⁴ However, Rule 902(14) now allows this to be done well before trial and enables the authentication of the evidence while barring any objection from opposing counsel.¹¹⁵

With these new amendments in place as of December 2017, many aspects of the Federal Rules of Evidence have been altered to accommodate ESI. The specific focus of this Note has been the authentication issue revolving around ESI. Much has been written here and elsewhere as to why the use of ESI in litigation is such a financial and time-consuming burden, but have these amendments done enough to

108. See FED. R. EVID. 902(13)–(14).

109. Grimm, *supra* note 93, at 721.

110. *Id.*

111. See *id.* at 718–19.

112. *Id.*

113. Lampley, *supra* note 96, at 531–32.

114. See *id.*

115. FED. R. EVID. 902(14) advisory committee's note to 2017 amendments.

resolve these problems? The answer is that same repeated law school phrase: “it depends.”

These amendments are still very new, but they will likely have a positive influence on authenticating ESI. In a situation where one party offers a relatively routine type of electronic data as evidence and the other party does not plan to challenge it, these amendments will save both sides time and money. They serve as a useful primer for the discussion of this Note. However, they are not the final solution. These amendments resolve only a niche set of circumstances. The answer cannot be to add self-authenticating provisions in an exhaustive list to all varieties of ESI. Technology will continue to advance, and attempting to make a comprehensive authentication list will only become a more complex proposition. Inevitably, the Rule amendments will lag behind the advancements in ESI usage as data storage further evolves.

One thing these amendments have not fixed is the chain of custody problem, which still exists. The chain of custody shows all the places a piece of evidence has been stored and who has had access to or control of the evidence, how it got to be stored where it is, and the condition it is in compared to its original form.¹¹⁶ Chain of custody becomes even more complex when dealing with ESI.¹¹⁷ The primary difference between ESI and paper documents is that ESI often deals with copies and almost never originals.¹¹⁸ A single file such as an email or PDF can be copied hundreds of times—through routine backups, for example—before it becomes relevant evidence. Each time a piece of ESI is copied, its integrity is threatened—authentication not only becomes more important, but also more difficult. When a piece of ESI must be certified, having it collected by a client or improperly transmitted between hardware systems could ruin the hash value or invalidate the accuracy of the system in which it was stored.¹¹⁹ Clients may unwittingly create such interference before they ever consult with an attorney. Unfortunately, once this chain has been “tampered” with, it may effectively be permanently broken.¹²⁰

In actuality, the solution to litigating with ESI cannot be contained within a rule change—the problems are not solely a product of antiquated rulemaking. An almost equal contributing factor lies in the antiquated practice methods of ESI. Too often, attorneys will request more

116. Helen Geib, *Chain of Custody and Its Critical Role in Authenticating Electronic Evidence*, QDISCOVERY, <https://qdiscovery.com/chain-of-custody-critical-role-authenticating-electronic-evidence/> (last visited Oct. 21, 2018).

117. *See id.*

118. *See id.*; DANIEL GARRIE & YOAV M. GRIVER, DISPUTE RESOLUTION AND E-DISCOVERY § 5:2 (2013).

119. *See* U.S. DEP’T OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 11 (1994), <https://www.ncjrs.gov/pdffiles1/nij/199408.pdf>.

120. *See* Busen, *supra* note 89.

e-discovery documents than they require to elevate costs of litigation.¹²¹ Parties will also challenge the obvious authenticity of evidence to force opposing counsel to prepare and present a witness.¹²²

The resolution must come from a more comprehensive and fundamental approach to the treatment of ESI. These rules represent the end handling of ESI when the emphasis should be more on the preliminary phases of authentication. Companies who frequently endure litigation and already direct large amounts of funds to the use of ESI can take several steps to avoid authentication issues.

One of the most important steps that a company can take is to create a team of people trained to handle ESI. With so many complexities to the preservation and use of ESI, a team with diverse expertise could better approach the task. Members from the information technology department, legal offices, and management can all offer insight into this process. Anyone who handles ESI without expertise could invalidate easy methods of authentication, so this team could reduce the risk of mishandling or ruining ESI.

As part of this team's responsibilities, the team members should create a written policy for the proper storing of ESI. The moving, copying, or collection of ESI should be monitored and tracked by an appointed employee. These uses should be recorded either in written form or through software designed to make similar recordings. The rights to alter or forward emails can be managed to prevent email tampering or distribution to unauthorized personnel, which would diminish authenticity.¹²³ Similarly, systems such as Microsoft Azure Information Protection keep backup files secure and reliable on a cloud server so that copies can be accurately compared to the stored originals for authentication.¹²⁴ Further, companies should be concerned with the security of their ESI and future review processes. Finally, firewalls and

121. See Jayme L. Walker & Tilak Gupta, *E-Discovery for Plaintiffs' Lawyers*, PLAINTIFF, Nov. 2015, at 39, <https://www.plaintiffmagazine.com/images/issues/2015/11-november/Plaintiff-Nov15-issue.pdf>.

122. See Busen, *supra* note 89.

123. ORACLE, INFORMATION RIGHTS MANAGEMENT—MANAGING INFORMATION EVERYWHERE IT IS STORED AND USED 10 (2009), <https://www.oracle.com/technetwork/middleware/webcenter/content/irm-10g-technical-whitepaper-129901.pdf>; Ajmal Kohgadai, *What Is Information Rights Management (IRM)?*, MCAFEE, <https://www.skyhighnetworks.com/cloud-security-blog/what-is-information-rights-management-irm/> (last visited May 14, 2019) (describing IRM as a category of software that allows assignment of permissions to certain employees for use of certain types of ESI within a company).

124. See LOGIKCULL, THE ULTIMATE GUIDE TO EDISCOVERY 47, 52, <https://www.logikcull.com/public/files/The-Ultimate-Guide-to-eDiscovery.pdf> (last visited June 9, 2019).

antivirus software can be employed to prevent outside intrusion into ESI and maintain its reliability.¹²⁵

Companies should look at how and where their ESI is being stored to effectively tailor these protections and procedures to the specific medium being used. For example, documents accessible to the internet should be given protections like Network Access Protection (NAP) to ensure they are not corrupted.¹²⁶ Meanwhile, ESI stored on disks or portable hard drives should use the most secure file systems.¹²⁷

One of the most difficult aspects of ESI is related to how difficult it can be to review the sheer volume of all the available documents.¹²⁸ Today, there are several different data forensic programs developed for the specific purpose of reviewing ESI electronically to reduce the cost and time it takes when documents are requested in discovery.¹²⁹ Some of these programs, such as LexisNexis Concordance, use keyword searches to quickly scan stored ESI.¹³⁰ When companies have made use of these types of services, courts have been more lenient and taken a reasonableness approach to the errors made when presenting all relevant ESI.¹³¹

One final solution involves coordination. As courts have begun to use a more case-by-case analysis of what is reasonable for accessibility and authentication,¹³² companies should begin creating definitive boundaries for themselves. Similar industries should join one another in creating standards for the maintenance and use of ESI. In this way, a court may look more favorably upon ESI stored in compliance with these standards and be more likely to accept authentication proof for all types of ESI.¹³³ These industry guidelines would also help reduce the costs involved with ESI by eliminating disputes over authentication objections. Such coordination is not uncharted territory. Medical societies and the

125. Deb Shinder, *Documenting Authenticity of Evidence for the E-Discovery Process*, TECHGENIX (July 16, 2008), <http://techgenix.com/documenting-authenticity-evidence-e-discovery-process/>.

126. *See id.*

127. *Id.*

128. *See* GARRIE & GRIVER, *supra* note 118.

129. *See* *What Is eDiscovery Software?*, LOGIKCULL, <https://www.logikcull.com/what-is-ediscovery-software> (last visited June 9, 2019).

130. *See* *Faster, Easier E-Discovery Review: The New Concordance Desktop*, LEXISNEXIS (Feb. 1, 2016), <http://businessoflawblog.com/2016/02/ediscovery-concordance-desktop/>.

131. *See* Steven Bennett, *E-Discovery: Reasonable Search, Proportionality, Cooperation, and Advancing Technology*, 30 JOHN MARSHALL J. INFO. TECH. & PRIVACY L. 433, 453, 463 (2014).

132. *See id.* at 435 n.8.

133. *See id.* at 453, 463.

respective bar association committees have joined to create guidelines for the admission and use of medical experts and evidence in trials.¹³⁴

CONCLUSION

The authentication of ESI is not a new challenge. Since the creation of digital information, the laws governing it have been struggling to keep up. It is simply too difficult for the rulemaking process to grow and evolve at the same rate as technology. The 2006 amendments marked an acknowledgement of the new form of paperless documents; the 2017 amendments are a concession to their growing prevalence.

As courts begin to implement these amendments and the full breadth of their impact becomes clear, litigators must also change. The proposed methods of use for the 2017 amendments discussed in this Note constitute the first step in solving ESI authentication challenges. However, the strategies given in the final portion of this Note describe a culture shift in how companies and their respective counsel use ESI. Understanding the unconventionality of ESI and its growing impact should be a goal of every litigation firm and is the main purpose of this Note.

134. *See generally* N.C. BAR ASS'N MEDICO-LEGAL LIAISON COMM., MEDICO-LEGAL GUIDELINES (2014), <https://www.ncmedsoc.org/wp-content/uploads/2013/06/Medico-Legal-Guidelines-2014.pdf>.