The Next Frontier in Drone Law: Liability for Cybersecurity Negligence and Data Breaches for UAS Operators

JOSEPH J. VACEK*

ABSTRACT

While questions related to UAS operations and use in government surveillance have been discussed at length, the legal ramifications of cybersecurity negligence and data breaches for UAS operators have yet to be addressed. In Part I, this article seeks to explore those areas by discussing the UAS data chain. Vulnerabilities in this data chain specific to UAS and in general are explored, followed by an examination of the state of the law related to the collection, use, retention, and dissemination of data. Part I concludes with an overview of current voluntary "Best Practice" documents offering guidance for collecting and managing data. Part II of this article applies Article III standing requirements and third-party liability limitations to the cybersecurity negligence and data breach issues. Existing federal law does not address liability for cybersecurity negligence or data breaches in UAS operations. This, combined with current interpretations of Article III standing requirements and a lack of a required standard of care for UAS operators to protect against cyber attack by third parties, results in the lack of a legal remedy for people whose private data is captured by drone and later compromised

* Joseph J. Vacek, J.D. is a tenured associate professor at UND Aerospace. He teaches aviation law, space law, and aviation technical and policy classes at the undergraduate, honors, and graduate levels. The author's primary research relates to UAS (drones) in the field of aviation law, including remote sensing, constitutional law related to search and seizure, privacy and data security, and civil issues such as tort and insurance law. He holds commercial pilot and certified flight instructor certificates and is a practicing lawyer, a former Peace Corps volunteer, and an entrepreneur. He is the faculty advisor for the UND competition aerobatic flying team. The author thanks the Campbell Law Review for excellent assistance and professionalism throughout the editing process for this Article. Specifically, Landon Van Winkle, Chief Articles Editor, demonstrated truly excellent legal and scholarly work in the editing process. It has been truly an honor to engage in thought with him and his team, the next generation in our learned profession.

in a cybersecurity breach. Thus, it appears UAS operators are effectively shielded from liability for data breaches beyond the UAS operation and in flight data collection.

INTRODUCTION

Over the last five years, Unmanned Aircraft System ("UAS") use by amateurs, journalists, businesses, and governmental actors has increased exponentially.[1] Their activities have resulted in the production of very large quantities of private or sensitive imagery and an uncountable accumulation of data related to such imagery.[2] Specifically, imagery from

1. The capabilities of UAS as cheap, efficient platforms upon which various remote sensing equipment can be mounted has led to the exponential increase in use. *See* Craigi, *The Drone Report 2016*, DRONE FLYERS (Aug. 21, 2015), http://www.droneflyers.com/2015/08/the-drone-report-2016/ [https://perma.cc/6FUD-8K9Z].

2. *See* Craigi, *Best Selling Camera Drones on Amazon – December 2016*, DRONE FLYERS (Dec. 1, 2016), http://www.droneflyers.com/2016/12/best-selling-camera-drones-amazon-december-2016/ [https://perma.cc/ZB8F-7STE] (estimating that DJI, which holds approximately 75% of the market share in consumer drones, will see sales of its drones top 1.5 million units in 2016-2017); Leo Sun, *Should Xiaomi be Worth More than DJI Innovations?*, MOTLEY FOOL (Jul. 12, 2016), http://www.fool.com/investing/2016/07/12/should-xiaomi-be-worth-more-than-dji-innovations.aspx [https://perma.cc/4RV5-J3DP] (calling DJI Innovations the "biggest drone maker in the world," estimating its market value

UAS platforms can include images or video in startlingly high-definition, offering a valuable perspective to enthusiasts, businesses, and government agencies.[3] For example, UAS imagery has been used by animal rights organizations to monitor hunters,[4] by the film industry to capture new perspectives,[5] and by law enforcement operations to apprehend criminal suspects.[6] Along with imagery, associated data—such as GPS coordinates of the imagery, or network traffic—can be gathered through UAS use.[7]

Such activities were rather limited until late 2016. Prior to August 29, 2016, drone operators needed either a "certificate of authorization"[8] or an exemption[9] from regular flight regulations to fly legally and avoid civil and criminal penalties. This changed on August 29, 2016, when Federal

---

at $8 billion, and further noting that DJI employs some 5,000 people worldwide and reported 2014 gross revenues of $500 million).

3. *See, e.g.*, Lindsey T. Anderson, Note, *The Sky's the Limit: UAS Regulations and Changing Applications in Agriculture*, 8 KY. J. EQUINE, AGRIC. & NAT'L RESOURCE L. 401, 405–06 (2015-2016) (discussing current uses of UAS, including "law enforcement, firefighting, border patrol, disaster relief, search and rescue, and military training[,]" by BP to monitor an oil pipeline in Alaska, and by film production firms in Hollywood for aerial shots on movie sets). *See also id.* at 410–12 (discussing the future application of UAS technology in precision agriculture, including monitoring fields for overwatering, pesticide overuse or deficiency, as well as instant assessment of crop damage following heavy rains in flooded fields); GLENNON J. HARRISON, CONG. RESEARCH SERV. R42938, UNMANNED AIRCRAFT SYSTEMS (UAS): MANUFACTURING TRENDS 5 tbl.1 (2013), https://fas.org/sgp/crs/natsec/R42938.pdf [https://perma.cc/UH45-3BS2] (listing twenty nonmilitary applications for UAS, including traffic monitoring, damage assessment, aerial photography, and sporting events coverage).

4. Alisa Mullins, *Hunters Watch Out: PETA's Drones Are Flying*, PETA (Oct. 21, 2013), http://www.peta.org/blog/hunters-watch-out-petas-drones-are-flying/ [https://perma.cc/7DK9-JPCC].

5. *See* AERIAL MOB, http://aerialmob.com/ [https://perma.cc/3JYG-S6XU].

6. Jennifer Lynch, *FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered*, ELECTRONIC FRONTIER FOUND. (Apr. 19, 2012), https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered [https://perma.cc/P5ZZ-WTXC].

7. Andy Greenberg, *Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones*, FORBES (July 28, 2011, 2:11 PM), http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/#1a6ff8a066f9 [https://perma.cc/UX43-HPH5] (discussing drones' potential for cell phone and wifi hacking).

8. *Certificates of Waiver or Authorization (COA)*, FED. AVIATION ADMIN., https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/ [https://perma.cc/YK99-WNMK] (last modified Aug. 19, 2016, 8:21 PM).

9. *See Section 333*, FED. AVIATION ADMIN., http://www.faa.gov/uas/beyond_the_basics/section_333/ [https://perma.cc/QAR6-JK2Q] (last modified Sept. 23, 2016, 9:46 AM) (explaining the exemption process set forth in Section 333 of the FAA Modernization and Reform Act of 2012).

Aviation Regulation part 107 went into effect.[10] A step towards integration of UAS into the National Airspace, part 107 created a straightforward licensure and regulatory structure allowing for commercial use of small unmanned aircraft.[11] The Association of Unmanned Vehicle Systems International, a trade group for the larger unmanned vehicle and robotics industry, predicts that in the first three years of integration more than 70,000 jobs will be created in the United States with an economic impact of more than $13.6 billion.[12] By 2025 an estimated 100,000 jobs, or more, will be created and integration will have an economic impact of $82 billion.[13] Most of that value will be tied directly to the data gathered by UAS operations.[14] However, along with the production of great value comes the production of very large quantities of sensitive imagery, data, and private information, much the same way Big Data companies such as Google or Facebook have created great value by aggregating large amounts of private data.[15] The issues related to the Big Data phenomenon have been

10. 14 C.F.R. § 107 (2016).

11. The regulations apply to the operation of "civil small unmanned aircraft systems within the United States." 14 C.F.R. § 107.1(a). Small unmanned aircraft systems are defined as those weighing less than 55 pounds at takeoff. *Id.* § 107.3. Several restrictions apply to the operation of authorized small UAS: they must be operated at altitudes of less than 400 feet, with limited exceptions, *id.* § 107.51(b); the operator must be in visual line of sight with the small UAS at all times, *id.* § 107.31(a); they may only be operated during daylight hours, *id.* § 107.29, away from clouds, *id.* § 107.51(d), and away from other aircraft, *id.* § 107.37. Further, the operator may not operate the small UAS in any controlled airspace, *id.* § 107.41, near any airport, *id.* § 107.43, or over any group of people, *id.* § 107.39.

12. DARRYL JENKINS & BIJAH VASIGH, ASS'N FOR UNMANNED VEHICLE SYS. INT'L, THE ECONOMIC IMPACT OF UNMANNED AIRCRAFT SYSTEMS INTEGRATION IN THE UNITED STATES 2 (2013), http://www.auvsi.org/auvsiresources/economicreport [https://perma.cc/7WKU-FQJA].

13. *Id.*

14. *See id.*; U.S. DEP'T OF TRANSP., UNMANNED AIRCRAFT SYSTEM (UAS) SERVICE DEMAND 2015–2035: LITERATURE REVIEW AND PROJECTIONS OF FUTURE USAGE 94 (2013), https://fas.org/irp/program/collect/service.pdf [https://perma.cc/3E88-FJWB] ("While most of the UAS industry is focused on a derivative of current military uses for security and police operations, the civil industry is looking to use the UAS as a platform to produce revenue from the data derived through the sensors.").

15. *See id.*; Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 824 tbl.3 (2015) (describing Google's cache of consumer web-browsing history data as more than 100 petabytes in size, while Facebook has amassed more than 300 petabytes of user data among posts, comments, and uploaded photos, and YouTube contains more than 1,000 petabytes of user-uploaded video content). *See also* Brian McKenna, *What does a petabyte look like?*, COMPUTERWEEKLY.COM (Mar. 2013), http://www.computerweekly.com/feature/What-does-a-petabyte-look-like [https://perma.cc/WL4X-HKFY] (describing one petabyte, or one thousand terabytes, as four times the

explored at some length and overlap significantly with the issues raised by UAS use for data gathering.[16] The key difference, however, is the length of the data chain and the consequent attenuation of potential liability for data breaches or negligence. This Article will explore, at length, this data chain and the limitations on liability. For purposes of this Article, the data chain[17] contains four links: (1) drone operation itself, (2) in-flight data collection, (3) post-flight data processing, and (4) data use, dissemination, and storage. Liability for data breaches in the last two links is well settled.[18] On the other hand, liability for data breaches in the first two links—drone operation and in-flight data collection—is unsettled, and the consequences of a breach there is likely different than in the latter two links. Thus, this Article explores liability for UAS operators and general data liability for post-flight activities.[19]

I. UAS USE FOR DATA GATHERING: LARGE QUANTITIES OF POTENTIALLY SENSITIVE IMAGERY, DATA, AND PRIVATE INFORMATION

Currently, a commercial UAS operator can gather imagery data and sell it largely without regulation.[20] A hypothetical example of such an activity follows: A real estate agency hires a UAS company to capture aerial imagery and video for use on the agency's website.

The UAS company uses a commercially available off-the-shelf quad-rotor drone system equipped with a stabilized high-definition camera.[21] Such a system is capable of about 15 to 30 minutes of sustained

---

amount of data collected by the U.S. Library of Congress from its inception until 2011, or "enough to store the DNA of the entire population of the US – and then clone them, twice.").

16. *E.g.*, Hu, *supra* note 15.

17. For purposes of this Article, I have organized UAS operations into a "chain" that begins with operating the drone and ends with uploading any data gathered in-flight to a personal computer, server, or other network-enabled device, in order to examine various vulnerabilities at each stage of the process.

18. *See infra* Part II.

19. An authorized small UAS operator is a person with a remote pilot certificate with a small UAS rating or a person manipulating the flight controls of the small UAS under the direct supervision of one so certified. 14 C.F.R. § 107.12(a) (2016).

20. Joseph J. Vacek, *Remote Sensing of Private Data by Drones is Mostly Unregulated: Reasonable Expectations of Privacy Are At Risk Absent Comprehensive Federal Legislation*, 90 N.D. L. REV. 463, 466 (2016).

21. This hypothetical example is based on the use of a DJI Phantom 4 drone, which is equipped with a 12 Megapixel camera and capable of recording 4k video (3840x2160) at up to 30 frames per second. *See Phantom 4 Specs*, DJI http://www.dji.com/phantom-4/info#specs [https://perma.cc/EGJ2-2AVQ] (last visited Dec. 17, 2016).

flight, which includes hovering, at altitudes of up to several thousand feet.[22] The electrically powered drone is both extremely agile and stable due to its gyroscopic autopilot.[23] The imagery gathered by its camera can be stored on-board or streamed live back down to the operator or another receiver and includes both high-definition video and still images.[24] The camera is fully gimballed, meaning it can remain focused and zoom-in on a subject of interest while the drone maneuvers.[25] Naturally, this drone is capable of trespassing onto private property, as its operator can fly it beyond the line of sight or even into a structure, using the drone's onboard GPS navigations system plus cameras to provide the operator with perspective.[26] The drone platform also makes quick work of gathering a bird's-eye view from practically any altitude, with the operator a mile or two away.[27]

The UAS company would be required to comply with all applicable flight-related regulations, such as altitude limitations,[28] exclusion from protected airspace,[29] and weather restrictions.[30] The real estate agency would have contracted with the UAS company to purchase the data gathered, including the intellectual property rights associated with the imagery and video. To differentiate itself, the UAS company advertises multi-spectral imagery,[31] which allows the real estate agency to capture a near-infrared thermal image, overlay it upon a visual image, and add the

22. *Id.* (the DJI Phantom 4 has a service ceiling of 19,685 feet above sea level).

23. *Id.* (the DJI Phantom 4 can travel at speeds up to 20 meters per second, or approximately 44 miles per hour, and can hover automatically at a fixed point for filming, with vertical and horizontal deviations at 0.1 and 0.3 meters, respectively).

24. *Id.* (the operator can view a "drones-eye" view on the ground in 720p video (1280x720) at 30 frames per second). *See also supra* note 21.

25. *Id.* (while the drone is traveling forward, the camera can pan and rotate freely, looking in any direction, from straight down to the ground to straight out to the horizon, and anywhere in between).

26. *Id. See also supra* note 24.

27. *Id.* (the remote control device can transmit and receive signals from the drone from up to 2.2 miles away).

28. 14 C.F.R. § 107.51(b) (2016).

29. *Id.* § 107.41.

30. *Id.* § 107.51(c).

31. *See, e.g.*, *Taking Flight: Small Business Utilization of Unmanned Aircraft: Hearing Before the H. Comm. on Small Bus.*, 114th Cong. 31 (2015) (statement of Michael J. Gilkey, CEO, 3D Aerial Solutions, LLC) ("The images record reflected sunlight at different wavelengths, or 'colors'. Different cameras are used to collect in different spectral bands (i.e. visible, near infrared and thermal infrared) to provide a variety of techniques for analysis. Multispectral cameras efficiently collect multiple colors simultaneously.").

result to the advertisement showing the house's energy efficiency level as a selling point.[32]

During the flight, the UAS company used near-infrared thermal imagery[33] and inadvertently captured high-definition imagery and video of a couple in the next yard sharing an intimate moment. The near-infrared camera recorded the scene even though a sunshade hid the couple from visual observation.[34] Neither the UAS company nor the real estate agency detected the error, and the agency later posted the images and video to its website. Soon thereafter, several "prurient interest" sites reposted the images. The couple was identified due to GPS location metadata associated with the imagery, ultimately causing the couple embarrassment and unwanted publicity.

Based on these hypothetical facts, a negligence lawsuit seems appropriate. However, the existing laws regulating remote sensing activities and data breaches suggest unexpected results in terms of liability for UAS-sensed data. To explain, this Article now turns to vulnerabilities in the data chain, followed by an exploration of the law related to the collection, use, retention, and dissemination of data gathered by UAS. Discussion turns next to limitations on liability for data breach and negligence in UAS cybersecurity before ultimately concluding that UAS operators are effectively insulated from liability for negligence in the data chain beyond flight activity.

A. Cybersecurity Vulnerabilities Throughout the Data Chain

Cybersecurity vulnerabilities exist throughout the data chain for UAS-sensed data.[35] As stated above, the data chain includes four links: (1) drone operation itself, (2) in-flight data collection, (3) post-flight data processing, and (4) data use, dissemination, and storage. Vulnerabilities in this data chain include sniffing, spoofing, snooping, and sabotage.[36] These

32. *See id.* at 70 (July 14, 2015 Letter from Nat'l Ass'n of Realtors) ("REALTORS® are excited about the potential to use UAS technology to take photographs and video footage of property listings for residential, commercial, and land sales or leases.").

33. *See* M. Annette Lanning, Note, *Thermal Surveillance: Do Infrared Eyes in the Sky Violate the Fourth Amendment?*, 52 WASH. & LEE L. REV. 1771, 1773–74 (1995) (discussing capabilities of forward-looking infrared (FLIR) imaging technology).

34. *See id.* at 1774 ("The FLIR can also detect body heat through a curtain or a thin partition." (citing State v. Young, 867 P.2d 593, 595 (Wash. 1994) (en banc))).

35. Aviation Rulemaking Advisory Committee—New Task, 80 Fed. Reg. 5880, 5880 (Feb. 3, 2015).

36. *See infra* Section I.A.2. *See also* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11 (2002) (discussing negligence liability in the context of distributed denial-of-service (DDoS) attacks); Kristin

vulnerabilities can occur in isolation or combination and may occur during flight operations or on the ground, with different ramifications for each situation.

1. Vulnerabilities Unique to UAS Operations

Each of the cybersecurity vulnerabilities may occur individually or in combination in the first link in the data chain. For starters, UAS are not entirely autonomous—all require some level of connection with the operator, whether it is a simple radio link directly connecting the controller with the aircraft flight controls[37] or a sophisticated three-way connection between the ground controller, the aircraft flight computer, and the GPS navigation satellite system.[38] A malicious actor can cause a loss of control by spoofing the controller or GPS signals with stronger, incorrect "spoofed" signals.[39] The malicious actor broadcasts false location data on the same GPS frequencies, which are relatively weak, so the drone relies on stronger false signals, resulting in position and navigation errors.[40] Drones that rely on GPS as part of their navigation or flight control systems are vulnerable to a spoofing attack in flight.[41] If the spoof is successful, the

---

Shields, *Cybersecurity: Recognizing the Risk and Protecting Against Attacks*, 19 N.C. BANKING INST. 345, 349–51 (2015) (discussing vulnerabilities in financial institution networks, including phishing, malware, and unauthorized access through unsecured third-party vendors); Jared Magill, *The Crooked Path to Determining Liability in Data Breach Cases*, WIRED, http://www.wired.com/insights/2015/03/crooked-path-determining-liability-data-breach-cases/ [https://perma.cc/88CE-KY5S] (discussing the history of cybercrime laws in the U.S. and the failed passage of the Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. § 101 (2014), which would have imposed criminal penalties on businesses entrusted with personally identifying consumer data that intentionally failed to disclose breaches of that data).

37. *See, e.g.*, John Patrick Pullen, *This Is How Drones Work*, TIME (Apr. 3, 2015), http://time.com/3769831/this-is-how-drones-work/ [https://perma.cc/E3GM-V4XQ].

38. *See, e.g.*, Alberto Cuadra & Craig Witlock, *How Drones Are Controlled*, THE WASHINGTON POST (June 20, 2014), http://www.washingtonpost.com/wp-srv/special/national/drone-crashes/how-drones-work/ [https://perma.cc/G7QD-B7PQ].

39. *See* Lorenzo Franceschi-Bicchierai, *Drone Hijacking? That's Just the Start of GPS Troubles*, WIRED (July 6, 2012, 6:30 AM), https://www.wired.com/2012/07/drone-hijacking/all/ [https://perma.cc/S6EV-SH66] (describing how, in a test conducted by researchers from the University of Texas and organized by the U.S. Department of Homeland Security, the researchers successfully hijacked a civilian drone by "spoofing" it with faulty GPS data).

40. *See id.* (explaining that GPS signals come from high altitude satellites which makes them highly susceptible to intentional and unintentional interference).

41. *See id.* ("The drone, an Adaptive Flight Hornet Mini, was hovering at around 60 feet, locked into a predetermined position guided by GPS. Then, with a device that cost around $1,000 and the help of sophisticated software that took four years to develop, the researchers sent a radio signal from a hilltop one kilometer away. In security lingo, they

UAS will follow the false signals and crash, resulting in a successful sabotage.[42] If a UAS operator experiences such a scenario, he would be potentially liable in tort for damages caused by the crash.[43]

Also related to the drone operation link in the chain, malicious actors might engage in packet sniffing. Packet sniffing is a software program or hardware device used to intercept and log data traffic that passes through it.[44] Any data that passes through a network, whether wired or wireless, can be vulnerable to a packet sniff, but not all packet sniffing is necessarily malicious.[45] However, malicious packet sniffing at the first link of drone operation can provide the initial information needed to hack the drone later or breach the data later in the data chain.[46]

The second link in the data chain, in-flight data collection, includes the capture of imagery or data from the drone operation by the drone's operator or, in the case of larger drones that have two person crews, a dedicated sensor systems operator. If the UAS operator in our hypothetical was streaming data from the UAS down to the controller and the data was unencrypted, it would be subject to sniffing and, potentially, snooping. A well-known vulnerability at the collection point of the data chain is simply not encrypting the data gathered.[47] If the drone broadcasts data to a ground

---

carried out a spoofing attack. 'We fooled the UAV (Unmanned Aerial Vehicle) into thinking that it was rising straight up,' says Todd Humphreys, assistant professor at the Radionavigation Laboratory at the University of Texas.").

42. *See, e.g.*, *id*. ("Deceiving the drone's GPS receiver, [the researchers] changed its perceived coordinates. To compensate, the small copter dove straight down, thinking it was returning to its programmed position. If not for a safety pilot intervening before the drone hit the ground, it would have crashed."). *See also* Brandon Bellows, Comment, *Floating Toward a Sky Near You: Unmanned Aircraft Systems and the Implications of the FAA Modernization and Reform Act of 2012*, 78 J. AIR L. & COM. 585, 608–09 (2013) (discussing the vulnerabilities of UAS to GPS spoofing attacks).

43. *See infra* Section II.B.

44. *See* Mani Potnuru, Note, *Limits of the Federal Wiretap Act's Ability to Protect Against Wi-Fi Sniffing*, 111 MICH. L. REV. 89, 91–92, 91 n.9 (2012) (explaining "passive" and "active" scanning for wireless signals and how those techniques are used by packet sniffers); Vacek, *supra* note 20, at 473 & n.51 (discussing packet analyzer software).

45. In fact, most Internet and Intranet (closed system) traffic is subjected to interception, mostly for network administration purposes of traffic management, security, or system health purposes.

46. *See* Potnuru, *supra* note 44, at 91–92 (explaining how packet-sniffing technology may be used to access sensitive information, which may then be used to facilitate other crimes).

47. *See, e.g.*, Geoffrey Christopher Rapp, *Unmanned Aerial Exposure: Civil Liability Concerns Arising from Domestic Law Enforcement Employment of Unmanned Aerial Systems*, 85 N.D. L. REV. 623, 631 (2009) ("[U]nencrypted video feeds captured by UAV optical sensors could be intercepted by private parties, who might seek to view the

receiver, anyone listening on the correct frequency can easily receive the data as well, much like public media broadcast over the airwaves. This is what happened in 2009 when Iraqi militants used cheap, off-the-shelf components to intercept video streamed from a U.S. Military Predator operation.[48]

As discussed below, the existing regulations for UAS operations are silent as to data captured. However, vulnerabilities begin at the moment of capture and operators may expose themselves to liability for not protecting potentially sensitive data.[49] Potential liability is complex due to issues with foreseeability, as discussed below, and a lack of applicable regulatory structure.[50]

2. General Cybersecurity Vulnerabilities

The third link in the data chain, post-flight data processing, opens the data to a multitude of general cybersecurity vulnerabilities, starting with packet sniffing on the ground. As previously discussed, packet sniffing is used to intercept and log data traffic that passes through a network.[51] Malicious packet sniffing can lead to the leak of sensitive data at this point in the data chain as well.

Spoofing refers to an attack on the data security later in the data chain.[52] Spoofing attacks usually involve a malicious actor attempting to

---

downloaded video or other imagery that exposes the targets of a UAV's sensor package to a loss of privacy.").

48. Siobhan Gorman, Yochi J. Dreazen & August Cole, *Insurgents Hack U.S. Drones*, THE WALL ST. J. (Dec. 17, 2009, 11:59 PM), http://www.wsj.com/articles/SB126102247889095011 [https://perma.cc/8RKJ-HKW7]; *see also* David Axe, *Iran Probably* Did *Capture a Secret U.S. Drone*, WIRED (Dec. 6, 2011), https://www.wired.com/2011/12/iran-did-capture-a-secret-u-s-drone/ [https://perma.cc/GDD7-JKR2] (discussing the reported Iranian recovery of a U.S. RQ-170 spy drone that crashed near the Iran-Afghanistan border, and speculating that Iran may have downed the drone by use of a signal jammer).

49. *See* discussion *infra* Part II.

50. *See infra* Section II.B.

51. *See supra* note 44 and accompanying text.

52. Spoofing refers to any cyber attack that uses, as a method, the substitution of false and malicious code or signals in place of the authentic code or signals with the intent that the victim remain unaware of the substitution. *See also* Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VAND. J. TRANSNAT'L L. 57, 77 n.89 (2010) ("Spoofing is defined as the 'appropriation of an authentic user's identity by non-authentic users, causing fraud or attempted fraud, in some cases, and causing critical infrastructure breakdowns in other cases. Spoofing can also target nonuserbased entities. For instance, an IP address can be spoofed to appropriate the identity of a server and not a human (user).'" (quoting BERNADETTE SCHELL & CLEMENS MARTIN, WEBSTER'S NEW WORLD HACKER DICTIONARY

access secure data by masquerading as a legitimate user.[53] They may do so either as an automated "man-in-the-middle" that inserts malicious code into a computer that is used later to disable or snoop, or as a "human spoof," where a person impersonates another who has legitimate access in order to obtain insider credentials and access a secure system.[54] The human "insider threat" is very difficult to protect against, since humans tend to trust other humans.[55]

Snooping is a sometimes sophisticated[56] method[57] of gathering and aggregating large quantities of user data.[58] While the term may refer to

289 (2006))). *Compare supra* notes 39–41 and accompanying text (describing spoofing of a nonuserbased entity earlier in the data chain, where the "victim" of the spoofed data is the drone itself, which mistakes malicious signals for genuine signals), *with infra* note 53 (describing spoofing attacks later in the data chain, where the victim is a human user who mistakes malicious code for the genuine article).

53. Douglas P. Whitlock, *Internet Fraud: Preventing and Responding to Phishing and Spoofing Scams*, 49 N.H. B.J. 30, 30 (2008) ("A spoof website uses the logos, content, and general design of the legitimate institution it is impersonating in order to trick the visitor into believing that he or she has linked to the legitimate website.").

54. *See* Shields, *supra* note 36, at 349–51, 350 (discussing third-party vulnerability and the Target data breach, where "cybercriminals accessed Target's computer system through the security system of a heating and cooling contractor who was working for Target." Because Target's system saw the HVAC contractor's system as a trusted user, the criminals were able to gain access to the Target system and install their malware); NIELS FERGUSON, BRUCE SCHNEIER, & TADAYOSHI KOHNO, CRYPTOGRAPHY ENGINEERING 10 (2010) (discussing the human element of cyber attacks).

55. *See* FERGUSON, SCHNEIER & KOHNO, *supra* note 54, at 10 ("[M]any of the really harmful attacks are performed by insiders, and a firewall does not protect against insiders at all.").

56. Although it may be as simple as eavesdropping on unencrypted communications. *See supra* notes 52–53 and accompanying text.

57. Of course, these methods of exploiting vulnerabilities in the data chain are not mutually exclusive. For example, spyware, which is a form of snooping, is often installed on the target system through the use of spoofing, or fooling a user into clicking a link or downloading a file that contains malware. *See, e.g.*, Gable, *supra* note 52, at 82 ("Spoofing attacks are concentrated on impersonating a particular user or computer, usually in order to launch other types of attacks."). Similarly, phishing is used to effectuate a spoofing attack: the cybercriminals send out emails to multitudes of users who may do business with a certain bank, posing as the bank, and trick users into entering personal information into spoof websites or into clicking links that install malware on their systems, enabling further snooping attacks. *See, e.g.*, Shields, *supra* note 36, at 349 ("Phishing is when a cybercriminal sends an email, text, or pop-up message asking for personal or financial information."); *see also id.* at 350 ("After phishing compromises a user's computer, cybercriminals can install malware. . . . [which can be used to] monitor and control online activity, steal confidential information, and commit fraud." (footnote omitted)).

58. MICROSOFT TECHNET, *Common Types of Network Attacks*, https://technet.microsoft.com/en-us/library/cc959354.aspx [https://perma.cc/TF94-H47X] (last visited Dec.

legitimate statistical research on public data,[59] for this article's purposes it refers to malicious software that runs in the background to access data without permission.[60] Snooping can occur anywhere in the data chain, but for the purposes of analyzing it as a general cybersecurity vulnerability, this Article will examine snooping later in the data chain: in the data processing link, by theft or unauthorized use in the use and dissemination link, or later in the storage link.[61] The result is that data essentially "leaks" out of an otherwise secure system and is then used for malicious purposes.[62]

Sabotage, of course, can be the most damaging vulnerability. While difficult to effect in the flight operation phase, data sabotage can result in wholesale data destruction or the capture and malicious encryption of data later held for ransom and the dubious promise of un-encryption upon payment of the ransom.[63] Recent data-ransom targets typically include

17, 2016) ("When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping.").

59. For example, it should come as no surprise that a person's Internet Service Provider, or ISP, knows every website that person visits while online. *See, e.g.*, Lincoln Spector, *Is Your ISP Spying on You?*, PCWORLD (Sept. 3, 2012, 7:42 AM), http://www.pcworld.com/article/261752/is_your_isp_spying_on_you_.html [https://perma.cc/2E84-PGKS] ("Your Internet service provider tracks what IP addresses you contact, which effectively means they know the web sites you're visiting. They can also read anything you send over the Internet that isn't encrypted."). *See also* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1438 ("How much personal information flows through an ISP's wires and is stored on its computers? In modern connected life, almost no other entity can access as much personal information.").

60. Jason Krause, *Beware of Spyware: Litigants Sometimes Resort to Computer Snooping, But It Could be a Crime*, 91 A.B.A. J. 57, 59 (2005) ("Software that spies on a person's computer is easy to install and very difficult to detect.").

61. For example, in our hypothetical, once the UAS company uploads the video onto its system, it would be vulnerable to a snooping attack, even before it was transmitted to the real estate agency if, for example, the UAS company had unwittingly installed spyware onto its system.

62. While snooping is typically associated with malicious software, or "spyware," snooping may also be done using hardware, which may be harder to detect. *See* Krause, *supra* note 60, at 55 (describing the "KeyKatcher," a keylogging snooping device that plugs in between the keyboard and computer, as "so small and innocuous it looks like part of the keyboard PS2 connector.").

63. *See, e.g.*, Robert McMillan, *In the Bitcoin Era, Ransomware Attacks Surge*, WALL ST. J. (Aug. 19, 2016, 11:59 PM), http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632 [https://perma.cc/9XML-TKV2] (describing one victim's payment of $500 in Bitcoin to hackers in order to unencrypt his Excel and Word documents that the hackers had maliciously encrypted by use of a virus or other malware).

hospital and patient records,[64] but imagery and data gathered by drones could easily be subject to the same scheme.[65] To return to our hypothetical and adjust it slightly, if the data processors withheld the images and video of the couple's intimate moments from public publication, the images would still be vulnerable to a sabotage (or ransom) attack if hackers managed to access the stored data and get the images.

The fourth link in the data chain includes data use, dissemination, and storage. Like the third link, data in use, dissemination, or storage is vulnerable to a multitude of cyber attacks, either human or bot-based, starting with software or hardware-based packet sniffing that usually leads to either a spoof attack or a continuous snooping attack facilitated by malicious software installed on the user's processor or storage device.[66] Data sabotage is a vulnerability in the fourth link as well.[67] Akin to a human virus or disease pandemic, more travel and human contact correlates to a higher infection rate; similarly, the more a dataset or information packet travels and the more Internet contact occurs, the higher the exposure to software viruses or malware.[68]

The cybersecurity vulnerabilities just discussed are neither novel nor solely a problem in the UAS industry, but they raise interesting questions because of the leveraged data gathering capabilities drones provide.

B. Lack of Regulation for Collection, Use, Retention, and Dissemination of Imagery, Data, and Information by UAS

The regulatory scheme for aviation activities and consequent liability for negligence in aviation operations is well established.[69] Two primary

64. Kaveh Waddell, *A Hospital Paralyzed by Hackers*, THE ATLANTIC (Feb. 17, 2016) http://www.theatlantic.com/technology/archive/2016/02/hackers-are-holding-a-hospitals-patient-data-ransom/463008/ [https://perma.cc/AQA4-AGZG].

65. Indeed this is increasingly likely as ransomware attacks have been rising at an alarming rate. *See* McMillan, *supra* note 63 ("According to the U.S. Department of Justice, ransomware attacks have quadrupled this year from a year ago, averaging 4,000 a day.").

66. Because the use, dissemination, and storage of the data subjects it to the same computing platforms and network vulnerabilities as the post-data flight processing that occurs in the third link, the vulnerabilities are largely the same. *See supra* notes 52–65 and accompanying text.

67. *See supra* notes 63–65 and accompanying text.

68. This vulnerability makes sense when one considers the structure of the internet. As data travels from host computer to host computer, it is subject to potential compromise or infection at each step.

69. *See* Mgmt. Activities Inc. v. United States, 21 F. Supp. 2d 1157 (C.D. Cal. 1998) (providing a comprehensive aggregation of the duties of care and law applicable to aviators); Merritt v. Shuttle, Inc., 187 F.3d 263, 268–70 (2d Cir. 1999) (discussing appellate subject matter jurisdiction as appropriate in aviation matters).

factors contributed to a regulatory and legal regime that supports one of the statistically safest industries—air transportation—in the domestic United States.[70] First, the enabling statutory language for the Federal Aviation Administration ("FAA") requires the agency to consider safety first, above all other considerations.[71] Second, the aviation administrative law system enforces aviation regulations under the principle of "safety first" while following *Chevron*'s[72] deference to the FAA.[73] FAA enforcement actions are subject to independent judicial review by an administrative law judge (ALJ), the National Transportation Safety Board (N.T.S.B.),[74] and finally, the federal courts.[75]

In 2014, the N.T.S.B., in *Huerta v. Pirker*, established that UAS are, in fact, aircraft subject to FAA regulation.[76] The FAA Administrator assessed a $10,000 fine against respondent Raphael Pirker in 2012 for Pirker's allegedly negligent or reckless operation of a Ritewing Zephyr drone near the campus of the University of Virginia, which violated existing FAA regulations.[77] Pirker was accused of flying the drone within ten feet of the ground, at altitudes up to 1,500 feet, through a traffic-filled tunnel, and within 100 feet of an active heliport. Pirker allegedly used the drone to run down a pedestrian on the sidewalk such that the hapless individual was forced to "take immediate evasive maneuvers so as to avoid being struck by the aircraft."[78] Pirker moved to dismiss the Administrator's Order of Assessment, arguing that the regulation he allegedly violated only applied to aircraft, but not to "model aircraft."[79] The ALJ agreed and

---

70. *How Aviation Safety Has Improved*, ALLIANZ, http://www.agcs.allianz.com/insights/expert-risk-articles/how-aviation-safety-has-improved/ [https://perma.cc/FG53-YSSN] (last visited Dec. 17, 2016).

71. 49 U.S.C. § 40104(a) (2012).

72. Chevron U.S.A., Inc. v. Nat. Res. Def. Council, 467 U.S. 837, 843 (1984) (holding that where Congress has delegated regulatory authority to a federal agency which has provided an administrative interpretation of an otherwise silent or ambiguous portion of a statute within which it has been delegated authority, "the question for the court is whether the agency's answer is based on a permissible construction of the statute.").

73. 49 C.F.R. § 821 (2016).

74. *Id.* § 821.2.

75. *Id.* § 821.64(a).

76. Huerta v. Pirker, N.T.S.B. Order No. EA-5730, 2014 WL 8095629, at *5 (N.T.S.B. Nov. 17, 2014) (granting *Chevron* deference to the FAA Administrator's prior interpretation of what constitutes an "aircraft" under 49 U.S.C. § 40102(a)(6) and 14 C.F.R. § 1.1).

77. *Id.* at *1. The regulation giving rise to the charge was 14 C.F.R. § 91.13(a) (2016), which proscribes, *inter alia*, operation of an aircraft "in a careless or reckless manner so as to endanger the life or property of another." *Id.*

78. *Huerta*, at *1 (quoting the complaint).

79. *Id.* at *8.

dismissed the Administrator's Order of Assessment.[80] The Administrator appealed to the N.T.S.B., which reversed the ALJ and held that "an 'aircraft' is any 'device' 'used for flight in the air.' This definition includes any aircraft, manned or unmanned, large or small."[81]

The robust existing system of aviation regulations, however, is silent as to regulating the data chain—the collection, use, retention, and dissemination of any imagery, data, or information gathered by UAS flight operations. The FAA simply has no statutory or adjudicated authority to regulate it. However, judging by the amount of time and effort devoted to discussing privacy issues related to UAS operations,[82] the industry and the FAA are clearly aware of the problem.

Even though the FAA has no authority to regulate the data chain, the agency continues to address it.[83] Incorporation by reference of a satisfactory privacy regulatory scheme would be effective. Incorporation of other federal statutes or regulations is not foreign to the Federal Aviation Regulations. For example, regulations on hazardous lithium batteries contained in the Hazardous Material Regulations section of the Code of Federal Regulations ("CFR") are incorporated into the Aviation CFR.[84] No suggestion of such an incorporation for data protection has been made either by the FAA or commentators. Therefore, it appears that a comprehensive regulatory structure for the data chain of remotely sensed data by drones does not exist.[85]

Federal laws regulating certain aspects of cybersecurity and the data chain do, of course, exist. The problem is that they set up only coarse, piecemeal regulation of remotely sensed data. The relevant existing federal laws related to remote sensing by drones include the Electronic Communications Privacy Act ("ECPA"),[86] the Privacy Act,[87] and even the Fourth Amendment of the United States Constitution.[88] The ECPA, which

80. *Id.* at *11.

81. *Id.* at *5 (quoting 14 C.F.R. § 1.1).

82. *See Press Release—DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems*, FEDERAL AVIATION ADMINISTRATION (June 21, 2016), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515 [https://perma.cc/4LJY-EH5K] (last visited Dec. 18, 2016).

83. *Id*.

84. 14 C.F.R. § 171.2(e).

85. Vacek, *supra* note 20.

86. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

87. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 § 3 (codified as amended at 5 U.S.C. § 552a (2012)).

88. U.S. CONST. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be

includes the Wiretap Act,[89] the Stored Communications Act,[90] and the Pen Register Act,[91] generally prohibits the unauthorized interception and use of the contents of electronic communications.[92] A drone equipped with remote sensing equipment tuned to eavesdrop on a particular bandwidth would intercept electronic communication if it were eavesdropping on the content.[93] While the ECPA proscribes such activity, the prohibition does not apply to the interception of non-content, or metadata.[94] Metadata includes information similar to that found on the outside of a traditionally addressed and mailed private, sealed letter: the sender, receiver, their addresses, and the date of mailing.[95] Digital metadata can include routing information as well. Thus, since the ECPA addresses only one potential use of UAS, it ceases to apply once data is gathered in the first and second links of the data chain.

Applicable to data further down the chain is the Stored Communications Act ("SCA"),[96] which, through the ECPA, protects data

---

violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

89. Omnibus Crime Control and Safe Streets Act of 1968, tit. 3, sec. 802, §§ 2510–2520 (codified as amended at 18 U.S.C. § 2510–2522).

90. Electronic Communications Privacy Act § 201 (codified at 18 U.S.C. §§ 2701–2710).

91. Electronic Communications Privacy Act § 301 (codified at 18 U.S.C. §§ 3121–3126).

92. 18 U.S.C. § 2510.

93. "'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." § 2510(12).

94. *See* Vacek, *supra* note 20, at 471 n.33 ("Metadata is data that describes other data, which includes structural information and descriptive information.").

95. This is distinguished from *content* data, or the contents *inside* the hypothetical envelope. "Contents" is a defined term under the ECPA, which means "when used with respect to any wire, oral, or electronic communication, includes any information concerning the *substance, purport, or meaning of that communication*." 18 U.S.C. § 2510(8) (emphasis added). This distinction is significant because certain provisions of the ECPA proscribe only the disclosure of *contents* of wire, oral, or electronic communications, and thus, by negative implication, do not apply to the disclosure of metadata. *See, e.g.*, § 2702(a)(1) ("a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity *the contents of a communication* while in electronic storage by that service . . . ." (emphasis added)); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1221 (2004) ("§ 2702 has slightly different exceptions depending on whether the information to be voluntarily disclosed consists of content or noncontent information.").

96. §§ 2701–2710.

stored on a server. While the ECPA generally protects data in transit, the SCA aims to prevent unauthorized access to data stored by third-party providers.[97] The statute is considered overly complex, and there is some discussion of what exactly constitutes "stored communications" depending on length of time the data remains on a particular server, whether it is opened or not, and whether the communication is deemed "content" or "non-content."[98] Generally speaking, however, the SCA is likely the most relevant federal law to illuminate the data chain problem presented here. Given the statutory duty of care imposed on data storage providers,[99] its narrow definitions only apply to a few applications of UAS gathered data.[100] This leads to an important distinction: Data voluntarily provided to an aggregator, such as a Facebook user sharing private information about a romantic experience, is subject to the contractual terms of the user agreement.[101] Therefore, Facebook does not violate the SCA through disclosures of that data if made pursuant to the terms of its user agreement, to the extent that those terms are lawful.[102] Such user agreements often provide consent for the aggregators to use the data in a multitude of ways.[103] For UAS-gathered data, such as our hypothetical couple's intimate moment, there is no such user agreement and no such consent given. Absent the knowing disclosure of information by the electronic

97. *Id*.

98. *See, e.g.*, Kerr, *supra* note 95, at 1227–28.

99. Albeit only in narrowly defined circumstances, assuming such data provider is a "public" provider, since the SCA has been held by implication not to apply to "nonpublic providers," Andersen Consulting, LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998) ("[T]he statute covers any entity that provides electronic communication service (e.g., e-mail) to the community at large."), and only in the event that voluntary disclosure by the provider is not permissible pursuant to one of the many statutory exceptions to the SCA, § 2702(b).

100. First, § 2702 only applies to *public* data providers. *See supra* note 99. Second, the prohibition on voluntary disclosure in § 2702(a) does not apply to the voluntary disclosure of non-content data, or metadata, as discussed *supra* notes 94–95 and accompanying text. Finally, even content data may be voluntarily disclosed with the user's consent. § 2702(b)(3).

101. *See* Daniel D. Barnhizer, *Propertization Metaphors for Bargaining Power and Control of the Self in the Information Age*, 54 CLEV. ST. L. REV. 69, 79–81 (2006) (arguing that, in the face of increasingly overbearing contracts of adhesion in the Internet context, consumer data should be recognized as a property right and either protected as such or held to be inalienable as a matter of law).

102. § 2702(b)(3) (providing that public providers may voluntarily disclose the contents of a communication "with the lawful consent of the originator . . . .").

103. *See, e.g.*, FACEBOOK, https://www.facebook.com/terms [https://perma.cc/7X7D-CH8F] (last visited Dec. 18, 2016).

communication service provider, the narrow protections offered by the SCA are not helpful in most data breach situations.

Continuing with the issue of consent, Congress enacted the Privacy Act of 1974 to set limits on federal agencies' collection, maintenance, use, and dissemination of personally identifiable information about individuals.[104] As codified, the act contains twelve exceptions allowing disclosure of data without consent.[105] The relevant exceptions for liability for cybersecurity issues include a "need to know" within an agency,[106] "routine uses,"[107] and law enforcement requests.[108] Those exceptions only apply to government agency use, however. Much more commonplace collectors, maintainers, users, and disseminators of data are commercial entities such as Google, Facebook, LexisNexis, and Thomson Reuters. The Privacy Act does not apply to private companies such as those listed.[109] Therefore, users of private data services do not enjoy any federal protections under the Privacy Act or under the Stored Communication Act if they have waived those rights in user agreements.

Finally, given recent decisions about consensual release of data, even the Fourth Amendment and remote sensing cases fail to establish a comprehensive structure to adequately address the data chain problem.[110] In *United States v. Skinner*, law enforcement tracked the defendant's location information, broadcasted from his mobile phone, without a search warrant.[111] The defendant argued that the Fourth Amendment prohibits such warrantless tracking as unreasonable.[112] The Court held that mobile

104. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 § 2(b)(1)-(2) ("The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to–(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies; (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent . . . .").

105. *See* 5 U.S.C. § 552a(b).

106. § 552a(b)(1).

107. § 552a(b)(3).

108. § 552a(b)(7).

109. *See* § 522a(b) ("No *agency* shall disclose any record . . . .") (emphasis added)); § 552a(a)(1) (incorporating the definition of agency as codified in 5 U.S.C. § 522); 18 U.S.C. § 522(f)(1) (defining "agency" as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency").

110. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012).

111. *Id*. at 775.

112. *Id*. at 777.

phone users have no "reasonable expectation of privacy in the data given off" by their devices.[113] Other relevant remote sensing cases include *Florida v. Jardines*, in which the Court compared a drug-sniffing dog's nose to a remote sensor,[114] and *United States v. Jones*, in which the Court prohibited the warrantless use of a GPS tracker on a suspect's vehicle.[115] However, in both *Jardines* and *Jones*, the Court held that Fourth Amendment searches occurred because of physical trespass.[116] When read together, those cases suggest that warrantless surveillance of metadata by law enforcement and governmental agencies is largely permitted so long as no physical intrusion occurs. This, along with the prevalence of "contracts of adhesion" by large companies requiring users to consent to third-party access of their data, together yield the result that citizens and consumers who use technology in even the most basic ways functionally waive control over their data.[117] Private data appears to have scant legal protection anywhere after the second link in the data chain.

Since federal law does not give meaningful protection to data gathered by drone, an injured plaintiff may turn to traditional tort law for a remedy. As with products liability, where manufacturers of products retain liability throughout the product's life, the question arises whether UAS operators, as "producers" of the data product, similarly retain liability. "The contractor who builds the scaffold invites the owner's workmen to use it. The manufacturer who sells the automobile to the retail dealer invites the dealer's customers to use it."[118] Does not the UAS operator who gathers the data invite the use of that data? The invitation may be to a specific person or an indeterminate class, "but in each case it is equally plain, and in each its consequences must be the same."[119] Should not the consequences of a data breach be attributable in some way to the producer of that data, like products liability?

---

113. *Id*.

114. Florida v. Jardines, 133 S. Ct. 1409, 1416–17 (2013).

115. United States v. Jones, 132 S. Ct. 945 (2012).

116. *Jardines*, 133 S. Ct. at 1417; *Jones* at 951–52.

117. *See, e.g.*, Barnhizer, *supra* note 101, at 71–72 ("The modern reality of highly sophisticated forms of adhesion contract—browse-wrap and click-wrap contracts—appears to exacerbate the lack of assent and take-it-or-leave-it nature of consumer adhesion contracts. As some commentators have noted, the fiction of consumer assent to such new forms of adhesion contracts is even more absurd than with their paper-based counterpart. Just as with the relatively crude paper-based contracts, few consumers ever bother to read these terms, and the nature of online contracting permits producers to hide their boilerplate terms far more effectively than even the finest of fine prints." (footnotes omitted)).

118. MacPherson v. Buick Motor Co., 111 N.E. 1050, 1054 (N.Y. 1916).

119. *Id*.

It appears that the rule of *MacPherson v. Buick Motor Company*—that a duty of care exists if a product reasonably expected to be dangerous is negligently made and is known to be used by those other than the original purchaser[120]—may have an exception for UAS data. Even though the sale of a data product would ordinarily be subject to products liability laws, liability for data breaches or negligence on the part of the original data gatherer (the UAS operator) is problematic due to attenuation.[121] Article III standing requirements and third-party liability limitations effectively leave potential plaintiffs without a remedy in tort because they may not be foreseeable users of UAS data or victims of its unauthorized dissemination.[122]

Unfortunately for the couple from our hypothetical, even a technological solution is not a viable protector of their private moments. Vulnerabilities in general,[123] in the software code used for flight controls or navigation,[124] and in data and server management[125] will persist as long as "informal code" is used.[126] "Informal code" describes the vast majority of software—it works well enough most of the time but might have bugs or errors.[127] On the other hand, "formal code," where computer logic is subject to mathematical proof at each step of an operation, results in each step of the software code returning a single possibility, closing the "backdoors" and bugs that cybercriminals exploit.[128] However, such secure technology comes at a significant price—slow processing speeds and huge amounts of necessary memory for the simplest operations.[129] Similarly,

120. *Id*.

121. *See infra* Part II.

122. *See infra* Part II.

123. *See* Kevin Hartnett, *Computer Scientists Close in on Perfect, Hack-Proof Code*, WIRED (Sept. 23, 2016, 8:00 PM), https://www.wired.com/2016/09/computer-scientists-close-perfect-hack-proof-code/ [https://perma.cc/5RAJ-9NKA].

124. Alan Kim et al., *Vulnerabilities Analysis for Unmanned Aerial Vehicles*, AM. INST. OF AERONAUTICS & ASTRONAUTICS, CYBER ATTACK 6–13 (2012), https://pdfs.semanticscholar.org/1a95/4775dd9a2596b7543af7693d707415077289.pdf [https://perma.cc/7DN3-NKHA].

125. Andrew V. Schmidt, Note, *Cyberterrorism: Combating the Aviation Industry's Vulnerability to Cyberattack*, 39 SUFFOLK TRANSNAT'L L. REV. 169, 181–84 (2016) (discussing cyber vulnerabilities in the aviation industry).

126. *See* Hartnett, *supra* note 123 (discussing informal and formal computer codes).

127. *See id.* ("[M]ost computer code . . . is written informally and evaluated based mainly on whether it works . . . .").

128. *Id.* ("[F]ormally verified software reads like a mathematical proof: Each statement follows logically from the preceding one. An entire program can be tested with the same certainty that mathematicians prove theorems.").

129. *Id.* ("[A] program that includes its formal verification information can be five times as long as a traditional program that was written to achieve the same end.").

blockchain authentication,[130] a cybersecurity protocol where each subsequent operation requires the verification of all prior operations, also requires significant computing power to run.[131] UAS are limited by weight due to aerodynamic considerations and limited in battery life due to those weight limitations.[132] Therefore, the use of small, lightweight processors, flight controllers, and sensors is necessary.[133] Small UAS simply cannot carry the batteries or computing power required to run formal code or block chain authentication.[134] Even if the energy or processing requirements were solved, the expense to do so is likely prohibitive.

Fears of privacy invasions, such as the involuntary exposure of the hypothetical couple's intimate moment, spurred President Obama to order an independent agency review of the lack of a privacy and data management regulatory structure as applied to UAS operations in 2015.[135] The process was conducted by the National Telecommunications Information Agency[136] and produced a concise best practices document,

130. Bitcoin uses block chain authentication to effectively prevent fraud. *See* Jay Schulman, *How Bitcoin Could Prevent Real Estate Fraud in Cook County*, CHICAGO (Dec. 9, 2016), http://www.chicagomag.com/city-life/December-2016/Cook-County-Bitcoin-Blockchain/ [https://perma.cc/2J9E-BCDE].

131. *See* Trevor I. Kiviat, Note, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 579 & n.70 (2015) (explaining that the blockchain validation system powering Bitcoin is dependent on the network participants' "computational power," which "essentially refers to how fast a machine can perform an operation.").

132. *See supra* notes 21–27 and accompanying text (describing limitations of a typical consumer-grade UAS).

133. The DJI Phantom 4, for example, weighs in at 1380 grams, or about 3 pounds. *See supra* notes 21–27 and accompanying text.

134. Recall that small UAS must have a combined takeoff weight of less than 55 pounds, *supra* note 11. Compare the 3-pound weight of the DJI Phantom 4 with that of the U.S. military's well-known Predator drone, which weighs 1,130 pounds when empty and takes off carrying up to 665 pounds of fuel and an additional 450 pound payload. U.S. AIR FORCE, *MQ-1B Predator* (Sept. 23, 2015), http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104469/mq-1b-predator.aspx [https://perma.cc/6BNR-NP4A].

135. Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, 80 Fed. Reg. 9355, 9357 (Feb. 20, 2015) [hereinafter Presidential Memo], https://www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03727.pdf [https://perma.cc/9VHV-AZSJ] ("There is hereby established a multi-stakeholder engagement process to develop and communicate best practices for privacy, accountability, and transparency issues regarding commercial and private UAS use in the NAS. The process will include stakeholders from the private sector.").

136. *Id*. ("Within 90 days of the date of this memorandum, the Department of Commerce, through the National Telecommunications and Information Administration, and in consultation with other interested agencies, will initiate this multi-stakeholder

which is discussed below.[137] Around the same time, various other federal agencies and private industry actors also produced their own best practices and internal guidance documents related to privacy and data chain management in UAS operations.[138] Together, these guidance documents may establish a duty of care for UAS operations.

C. Best Practices Documents for Collecting and Managing Sensitive or Private Data That Are Voluntary Only

A study conducting a broad review on commercial drone literature in research, magazine, and news databases from 2010 to 2015 identified key areas of social and ethical concerns related to commercial drone use.[139] The most frequently cited concern was in the area of law and regulation with privacy issues falling closely behind.[140] It is reasonable to conclude that concerns of law and regulation overlap both categories of flight operations as well as cybersecurity, since privacy issues would not be a relevant concern but for drones' abilities to conduct remote sensing activities of private activities. Similar concerns led UAS operators, including governmental operators,[141] universities,[142] and the industry itself,[143] to produce several guidance documents during the same timeframe that indicate a discipline-specific focus on the difficult questions of data privacy and cybersecurity. Taken together, these guidance documents may

---

engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS use.").

137. *See* Multistakeholders convened by Nat'l Telecomms. & Info. Admin., *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability* (2016) [hereinafter *Voluntary Best Practices*], https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf [https://perma.cc/97UH-GN3L].

138. *See, e.g.*, DEP'T OF HOMELAND SEC., WORKING GROUP TO SAFEGUARD PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN THE DEPARTMENT'S USE AND SUPPORT OF UNMANNED AERIAL SYSTEMS 2 (2012) [hereinafter DHS MEMO], https://www.dhs.gov/sites/default/files/publications/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information.pdf [https://perma.cc/3KSN-PXKE]; *Code of Conduct*, ASS'N FOR UNMANNED VEHICLE SYS. INT'L, [hereinafter *AUVSI Code of Conduct*] http://www.auvsi.org/content/conduct [https://perma.cc/CPN3-BBW5].

139. Rocci Luppicini & Arthur So, *A Technoethical Review of Commercial Drone Use in the Context of Governance, Ethics, and Privacy*, 46 TECH. IN SOC'Y 109, 111–12 (2016).

140. *Id.*

141. *See, e.g.*, DHS MEMO, *supra* note 138.

142. *See, e.g.*, U.N.D., *Committee on Unmanned Aircraft System Research Ethics & Privacy*, https://und.edu/research/resources/uas-research-ethics-privacy.cfm [https://perma.cc/EX4T-MNKP].

143. *AUVSI Code of Conduct*, *supra* note 138.

equip future courts with enough evidence of an industry-wide standard of care for UAS cybersecurity throughout the data chain.[144]

In the interim, the broader UAS industry had the opportunity to comment on a "best practices" forum hosted by the National Telecommunications and Information Administration (NTIA) pursuant to a 2015 Presidential Memorandum.[145] The Memorandum established UAS-specific guidelines for federal agencies to protect privacy, accountability, transparency, and reporting, including a requirement for agencies to "at least every 3 years, examine their existing UAS policies and procedures related to the collection, use, retention, and dissemination of information obtained by UAS . . . ."[146] The NTIA forum produced a "best practices" document intended to provide guidance to all UAS operators.[147] Even though the document itself claims that it is not intended to establish a standard of care or the basis for statutory or regulatory obligations, a court could find it does establish such a standard of care, in whole or in part, if sufficient evidence of use exists.[148] Part IV of the document, titled "Voluntary Best Practices,"[149] includes five elements directly applicable to privacy and data chain management.[150]

Overall, these best practices request that operators simply provide notice and act reasonably.[151] Upon closer examination, however, the best practices implicitly recognize the inherent privacy problem framed by this Article—that once gathered, data receives very little protection and potential plaintiffs have very little recourse. A footnote in the best practices document sums it up nicely: "These Best Practices recognize that UAS operators may not be able to predict all future use of data. Accordingly, these Best Practices do not intend to discourage unplanned or innovative data uses that may result in desirable economic or societal

144. *Voluntary Best Practices*, *supra* note 137.

145. Presidential Memo, *supra* note 135.

146. *Id.* at 9355–56.

147. *See Voluntary Best Practices*, *supra* note 137, at 5 ("These voluntary Best Practices for UAS focus on data collected via a UAS, which includes both commercial and non-commercial UAS.").

148. *Id.* at 2 ("In some cases, these Best Practices are meant to go beyond existing law and they do not—and are not meant to—create a legal standard of care by which the activities of any particular UAS operator should be judged.").

149. *Id.* at 5.

150. *Id*. at 5–6. These five elements are: (1) Inform others of your use of UAS; (2) Show care when operating UAS or collecting and storing covered data; (3) Limit the use and sharing of covered data; (4) Secure covered data; and (5) Monitor and comply with evolving federal, state, and local UAS laws. *Id.*

151. *See id.*

benefits."[152] This statement supports an inference that the "exciting possibilities that come with [UAS]" may trump the "responsible, ethical, and respectful" duties and "commitment to transparency, privacy, and accountability" outlined for UAS operators by the Voluntary Best Practices.[153]

Even if a court finds the duties and standards suggested by the Voluntary Best Practices have become a de facto standard of care for UAS remote sensing activities, existing law—including constitutional standing requirements and third-party liability limitations—probably limits UAS operators' liability for breaches in the data chain, depending on where in the data chain the breach occurs.

II. LIMITED LIABILITY FOR DATA BREACHES

The liability issues related to cybersecurity and database breaches have been discussed in terms of standing,[154] duty under tort law,[155] and in other contexts, such as security breaches of financial service providers,[156] and communication and user privacy in social media.[157] The legal principles that limit liability in those contexts apply similarly in UAS remote sensing and the data chain context.[158] Current standing requirements[159] as applied to data breaches frequently deprive potential plaintiffs of standing.[160] Third-party liability limitations also limit potential plaintiffs' abilities to sue, because well-established principles of tort law applied to data breach cases usually prevent recovery absent a business or

152. *Id*. at 5 n.3.

153. *Id.* at 2.

154. Arthur R. Vorbrodt, Note, Clapper *Dethroned: Imminent Injury and Standing for Data Breach Lawsuits in Light of Ashley Madison*, 73 WASH. & LEE L. REV. ONLINE 61 (2016).

155. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255 (2005).

156. Huggins v. Citibank, 585 S.E.2d 275 (S.C. 2003).

157. Christopher J. Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36 (2015).

158. *See infra* Section II.A.

159. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992) (discussing the three requirements for standing) (citations omitted); City of Los Angeles v. Lyons, 461 U.S. 95, 101–02 (1983) (discussing the injury requirement of standing) (citations omitted).

160. *See infra* Section II.A.

legal relationship, which is usually lacking between the UAS operator and the subject whose data is breached.[161]

A. Article III Standing Requirements: Precluding Negligence Lawsuits in Data Breach Cases

Whether a person injured by a data breach has constitutional standing has been addressed by multiple courts at the state and federal levels. The Seventh[162] and Ninth[163] Circuits answered in the affirmative, and the Third Circuit in the negative.[164] In *Clapper v. Amnesty International USA*, the Supreme Court addressed standing for future injuries comparable to those which may occur in data breach cases.[165] Commentators have interpreted *Clapper* to impose stricter requirements for standing: plaintiffs must be able to show future injury is "certainly impending."[166] Notwithstanding *Clapper*'s more stringent requirement, the majority also noted that standing may be available to plaintiffs showing a "substantial risk" of injury.[167] Requiring plaintiffs alleging future injuries from a data breach to meet a stricter requirement by showing an injury is "certainly impending" would effectively bar most data breach plaintiffs from proceeding.[168] On the other hand, applying the "substantial risk" standard would provide data breach plaintiffs an easier time showing injury in fact. Still, however, they must satisfy the other two elements of standing.

For plaintiffs alleging injury due to data breach caused by a snooping drone, the actual flight activity may be their only recourse—such as

---

161. *See generally, e.g.*, Durkee v. C.H. Robinson Worldwide, Inc., 765 F. Supp. 2d 742, 748 (W.D.N.C. 2011) ("The duty owed by a defendant to a plaintiff is determined by the relationship subsisting between them." (citing Kientz v. Carlton, 96 S.E.2d 14, 17 (N.C. 1957))); Durden v. United States, 736 F.3d 296, 304 (4th Cir. 2013) ("In general, there is neither a duty to control the actions of a third party, nor to protect another from a third party." (quoting Scadden v. Holt, 733 S.E.2d 90, 92 (N.C. Ct. App. 2012))). *See also infra* Section II.B.

162. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).

163. Robins v. Spokeo, Inc., 742 F.3d 409, 413 (9th Cir. 2014), *vacated and remanded*, 135 S. Ct. 1540, 1545 (May 16, 2016) (holding that the Ninth Circuit failed to consider in detail the particularity *and* concreteness of plaintiff's injury and accordingly remanded for analysis of both standing requirements).

164. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

165. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013).

166. Bradford C. Mank, Clapper v. Amnesty International: *Two or Three Competing Philosophies of Standing Law?*, 81 TENN. L. REV. 211, 214 (2014).

167. *Clapper*, 133 S. Ct. at 1150 n.5 (citations omitted).

168. *See, e.g.*, Mank, *supra* note 166; Whalen v. Michael Stores Inc., 153 F. Supp. 3d 577 (E.D.N.Y. 2015); Khan v. Children's Nat'l Health Sys., No. TDC-15-2125, 2016 U.S. Dist. LEXIS 66404, at *3–7 (D. Md. May 19, 2016).

trespass in our hypothetical couple's case. Showing "certainly impending" damages due to the leaked intimate videos would be more difficult than showing a "substantial risk" of injury. As the imagery and video become widely distributed on the Internet, the harm to the hypothetical couple's reputation may increase while, paradoxically, the legal harm becomes more attenuated. Data breach cases related to financial or identity fraud, such as that in *Reilly v. Ceridian Corp.*,[169] illustrate this phenomenon. In *Reilly*, the plaintiff's data, stored by defendant, was hacked.[170] The plaintiffs were notified of the breach and later sued, alleging risk of future harm.[171] The court held that mere allegation of future harm did not meet constitutional standing requirements, despite the cost incurred with monitoring credit.[172]

On the other hand, in *Remijas v. Neiman Marcus Group*, where hackers breached the retailer's database and stole customers' credit card numbers, the court found that costs directly associated with monitoring credit scores to guard against potential future fraud met the *Clapper* requirement for "certainly impending injury."[173] For our hypothetical couple, there would be no threat to their credit. Their privacy and reputation were injured but, absent financial repercussions, they would not meet the standing requirement.

Most recently, a district court suggested that standing exists in a data breach case when a plaintiff can show either: "(1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud."[174]

From these cases, it seems that unless a data breach specifically harms an individual financially, the footholds needed to scale the slope of standing would be absent[175] However, the vast majority of data breach plaintiffs do not articulate a direct legal or financial harm as a result of the

169. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

170. *Id.* at 40.

171. *Id.*

172. *Id.* at 43–46.

173. Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 697 (7th Cir. 2015).

174. Khan v. Children's Nat'l Health Sys., No. TDC-15-2125, 2016 U.S. Dist. LEXIS 66404, at *14 (D. Md. May 19, 2016).

175. Data breach plaintiffs tend to be single members of huge classes or single data points in huge databases. The data breach in *Reilly* affected approximately 27,000 people, 664 F.3d at 40, while the breach at issue in *Remijas* affected 350,000, 794 F.3d at 690. The 2013 Target Corp. breach affected an estimated 40 million consumers. Gregory Wallace, *Target Credit Card Hack: What You Need to Know*, CNN (Dec. 23, 2013, 11:43 AM), http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/ [https://perma.cc/RR4A-3GPP].

data breach.[176] Many do, of course, suffer attenuated harm, such as the hassle and expense of obtaining new credit cards, closing compromised accounts, or fixing inaccurate credit reports. But each link in the data chain further attenuates the harm with the eventual result that, legally, the injury becomes speculation.[177]

For those like our hypothetical couple who are injured by data breaches affecting their privacy, becoming an unwilling public figure on the Internet occurs after the first two links of the UAS data chain—drone operation and data processing. The UAS operator's liability for the flight ends there due to third-party limitations such as foreseeability in tort and lack of privity in contract.[178]

B. Third-Party Liability Limitations: Precluding Negligence Theory Against UAS Operators

The landmark case of *Palsgraf v. Long Island Railroad Co.* established the limits of a third-party's duty and directly applies to the data chain problem.[179] "The risk reasonably to be perceived defines the duty to be obeyed, and risk imports relation; it is risk to another or to others within the range of apprehension."[180] A reasonable person would likely feel apprehensive about a data breach compromising her sensitive information, and the first part of the *Palsgraf* rule suggests that entities managing the data chain would be liable for the risk of data breach as one that is "reasonable to be perceived." Under *Palsgraf*, a UAS operator must satisfy its duty of care for flight operations and data gathering by ensuring any

176. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007) (affirming dismissal of putative class action seeking relief for data breach because the class members had no compensable damages, chiefly because the court, faced with a novel question under Indiana law, believed that "Indiana law would not recognize the costs of credit monitoring that the plaintiffs seek to recover in this case as compensable damages.").

177. *See, e.g.*, *In re* Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1309 (D. Minn. 2014) (declining to dismiss class members' negligence claim against Target, related to the data breach mentioned *supra*, where class members argued that "Target's own conduct, in failing to maintain appropriate data security measures and in turning off some of the features of its security measures, created a foreseeable risk of the harm that occurred, and Plaintiffs were the foreseeable victims of that harm."). In the case of a UAS operator, like the one in our hypothetical who has no relationship to the victims, liability in negligence will turn on the foreseeability of the breach. It is arguably more foreseeable that a UAS will crash during flight and cause injury, or allow a passerby to recover an onboard camera and its contents, than it is that data captured from it will be hacked or exploited somewhere down the data chain.

178. *See supra* notes 162–77 and accompanying text.

179. *See* Palsgraf v. Long Island R.R. Co., 162 N.E. 99 (N.Y. 1928).

180. *Id.* at 100.

imagery or video streamed down from the aircraft to the remote operator is not inadvertently leaked, such as by broadcast on a public frequency. Since that is a known vulnerability in the flight and data gathering phases, it is likely a reasonably perceivable risk.[181] A data breach due to a public data transmission is likely a foreseeable event and thus would incur consequent liability for the UAS operator. A UAS operator, like the one that inadvertently captured the hypothetical couple's intimate moment, could probably refute a negligence claim by the couple that they had a duty to avoid capturing the intimate imagery. A UAS operator may reasonably claim to be in a similar position as the railroad in *Palsgraf*—unable to foresee the results of a photo lawfully taken several steps down the data chain—and argue that no duty runs back up the data chain from the plaintiff. Importantly, in *Palsgraf* there was a legal relationship between the parties—Ms. Palsgraf purchased a train ticket from the defendant railroad company.[182] A UAS operator engaged in remote sensing activities of third parties has no legal relationship with the third parties, and the lack of such a relationship would likely provide an effective defense to a negligence suit.

Second, most data breaches are the result of malicious criminal acts by third parties intent on stealing the data.[183] In this far more common scenario, *Kline v. 1500 Massachusetts Avenue Apartment Corp.* would apply, in which a landlord owed no duty "to provide protection commonly owed by [law enforcement]"[184] or to be "an insurer of the safety of his tenants."[185] Under *Kline*, the hypothetical UAS operator likewise has no common-law duty to protect the remotely sensed data from cybercriminal hacking attempts such as sniffing, snooping, or spoofing.

A database provider, like a landlord, owns server space where data is stored and would not, under *Kline*, have a duty to protect potential cybercrime victims against criminal cyber attack. Courts have directly addressed the question of whether there exists a common-law duty of care for data possessors to secure user data from theft by cybercriminals. In *Huggins v. Citibank*, the plaintiff sued the bank because a third-party cybercriminal opened a credit account in the plaintiff's name.[186] The

181. *See id.* at 100 (discussing foreseeability).

182. *Id.* at 99 ("Plaintiff was standing on a platform of defendant's railroad after buying a ticket to go to Rockaway Beach.").

183. VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 3 fig.3 (2016), http://sova.com/wp-content/uploads/2014/09/rp_DBIR_2016_Report_en_xg-1.pdf [https://perma.cc/T28F-3VS6].

184. Kline v. 1500 Mass. Ave. Apartment Corp., 439 F.2d 477, 487 (D.C. Cir. 1970).

185. *Id.*

186. Huggins v. Citibank, 585 S.E.2d. 275, 276 (S.C. 2003).

plaintiff alleged the bank had a minimal duty to protect the plaintiff by verifying the identity of the credit applicant before issuing the card.[187] The Court found that "in order for negligence liability to attach, the parties must have a relationship recognized by law as the foundation of a duty of care."[188] Most people would probably consider their financial data to be the most deserving of legal protection, but "[t]he relationship, if any, between [banks and victims of credit card fraud] is far too attenuated to rise to the level of a duty between them."[189] This line of reasoning extends to less sensitive areas of data privacy, such as software virus infections of home computers with a similar result.[190] Extending the analysis to UAS operators, *Huggins* creates similar results for our hypothetical couple—the UAS operator owes no duty of care to protect the couple's privacy because there is no legal relationship between the parties.

As a final note, it bears remembering that a contract may modify common-law duties of care.[191] A real estate agency may impose a duty upon UAS operators to take certain precautions with their customers' or third-party beneficiaries' data. Likewise, a contractual duty may require a server space provider to protect server users against criminal cyber attack. However, this Article focused on the default setting: the lack of a regulatory structure for data gathering by UAS and the potential common law liability between victims of data breaches and the UAS operator absent special relationships or contractual liability.

---

187. *Id.*

188. *Id*. at 277.

189. *Id*.

190. *See* Emily Kuwahara, Note, *Torts v. Contracts: Can Microsoft Be Held Liable to Home Consumers for its Security Flaws?*, 80 S. CAL. L. REV. 997, 1025–31 (2007) (arguing for an extension of products-liability law to cover software programs, invalidation of warranty disclaimers used by software companies, and an exception to the economic loss rule for software-related data breach losses).

191. Of course, depending on the facts, a breach of a contractual duty may give rise to a breach of contract action, rather than a cause of action sounding in negligence. *See, e.g.*, Lawyers Title Ins. Corp. v. Rex Title Corp., 282 F.3d 292, 293 (4th Cir. 2002) ("In general . . . Maryland does not recognize a cause of action for negligence arising solely from a contractual relationship between two parties." (citing Heckrotte v. Riddle, 168 A.2d 879, 882 (Md. 1961))). *But see* Eli Research, Inc. v. United Commc'ns Grp., LLC, 312 F. Supp. 2d 748, 758 (M.D.N.C. 2004) ("A duty to act for negligence purposes may flow from a contract or statute or may be implied from attendant circumstances." (citing Huyck Corp. v. C.C. Mangum, Inc., 309 S.E.2d 183, 187 (N.C. 1983))); Hardin v. York Mem'l Park, 730 S.E.2d 768, 776 (N.C. Ct. App. 2012) ("[A] duty of care may arise out of a contractual relationship, the theory being that accompanying every contract is a common-law duty to perform with ordinary care the thing agreed to be done, and that a negligent performance constitutes a tort as well as a breach of contract." (quoting Olympic Prods. Co. v. Roof Sys., Inc., 363 S.E.2d 367, 371 (N.C. Ct. App. 1988))).

CONCLUSION

Under current law, UAS operators are effectively relieved of liability for negligence in the data chain beyond flight activity. Existing federal law does not address liability for cybersecurity negligence or data breaches in UAS operations. Further, current interpretations of Article III standing requirements coupled with a lack of a required standard of care for UAS operators to protect against cyber attack by third parties. These realities result in the lack of a legal remedy for people whose private data is captured by drone and later compromised in a cybersecurity breach.

Data breach plaintiffs struggle to meet Article III standing requirements. Unless they can show more than an attenuated threat and meet the "concrete and particularized injury that is actual or imminent" or "certainly impending,"[192] they will not be able to state a claim that at some point in the data chain someone had at least a reasonable duty of care specific to the plaintiff and breached that duty, or even to argue the UAS operator produced a data product and should be liable under the *MacPherson* products liability rule.

For the hundreds of thousands of data breach victims[193] who cannot meet both the standing requirements and articulate a special duty of care, there is no remedy under current law. Neither the existing federal statutes governing data nor the Electronic Communications Privacy Act nor the common law provide an effective remedy to people whose data has been compromised.

From the perspective of UAS operators who, by virtue of their employment or business activities, are actively engaged in gathering data that has great value for both legitimate users and for hackers and digital miscreants, that same lack of remedy provides a welcome liability shield for liability beyond two links in the data chain: (1) the UAS operation and (2) in flight data collection. It appears UAS operators are also effectively shielded from liability for data breaches in the final two links in the data chain: (3) post-flight data processing, and (4) data use, dissemination, and storage.

192. *See supra* notes 169–72 and accompanying text.

193. *See supra* note 175.