Consumer Privacy in an Age of Commercial Unmanned Aircraft Systems

RYAN HAGEMANN

In recent years, the commercial potential of unmanned aircraft systems (UASs), more commonly referred to as drones, has captured the public imagination. From Amazon's ongoing testing of a UAS delivery service to Uber's recently proposed vertical take-off and landing transportation network, the commercial possibilities are ever growing.

To begin expediting the deployment of this emerging technology, in October 2017 the Trump administration issued a memorandum to the secretary of transportation directing the establishment of a UAS-integration pilot program (White House 2017). Although this is a notable step toward integrating and operationalizing UAS commercial operations in the national airspace, the privacy implications of this technology remain a pressing concern in many quarters.

UAS privacy issues are often framed in the context of government surveillance and potential First and Fourth Amendment violations. The implications for nongovernmental private-sector data collection, however, have received less attention. An "invasion" of privacy is heavily contextual, based on *who* is doing the surveilling, *how* it is carried out, for *what* purpose, and *where* it is conducted. For the discussion that follows, the *who* is specifically siloed to commercial service providers. The government's breach of an individual's privacy is subject to any number of statutory restrictions on law enforcement and intelligence agencies, not least of which include the Fourth Amendment to the

Ryan Hagemann is director of technology policy at the Niskanen Center.

The Independent Review, v. 23, n. 1, Summer 2018, ISSN 1086–1653, Copyright © 2018, pp. 9–22.

Constitution, and is far more clearly legally delineated. The *how, what,* and *where* of commercial "surveillance," however, are much less clear, especially in the context of UAS operations.

For the purposes of this paper, the focus on "surveillance" is specifically constrained to commercial UAS data-collection operations and nongovernmental surveillance that does not implicate constitutional considerations under the Fourth Amendment. I begin by discussing more general issues of privacy in the digital age as well as the domestic legal and regulatory structure that governs privacy. Then I examine these issues as they currently relate to UAS data collection for commercial purposes as well as the current debate over acquiring consent. The paper concludes by looking at all of these issues in the context of a hypothetical future-use scenario for commercial UAS data collection and argues that technology-specific regulations would be an ill-advised means of responding to potential privacy challenges.

How We (Paradoxically) Think about Privacy

Privacy is an amorphous concept. Its subjective valuation differs from individual to individual, and conventional expectations have changed considerably over time (Hagemann 2016). For example, in their seminal law review article "The Right to Privacy," Samuel Warren and Louis Brandeis argued that "[t]he intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury" (1890, 194). These concerns were specific to the emergence of a new technology at the end of the nineteenth century: the camera. Samuel Warren, taking great offense at the audacity of local photographers snapping pictures of his daughter's wedding on Boston Common, coauthored the article as a reply to concerning developments over the emergence of a new technology that held the potential to upend traditional sociocultural privacy norms. Such responses were and are nothing new.

These types of fears materialize at regular intervals throughout history and often subside as the new technology proves its utility to individuals. Such fears have been a common enough occurrence that they even have a name: the privacy panic cycle. This cycle is a social phenomenon in which the emergence of a new technology induces fear in a subset of the population. As Daniel Castro and Alan McQuinn have noted, these "techno-panics" result from fears that "center on an anticipated problem that does not come to pass. . . . While society eventually overcomes techno-panics, they can significantly slow the pace of technological progress, imposing real costs on society in the

process" (2015, 2). These cycles occur over time in four stages, distinguished by three inflection points of public concern.

The *trusted-beginnings* stage occurs when a technology is still emerging and remains a novelty. At a "point of panic," however, public concerns fuel the shift toward the *rising-panic* stage, during which public concern begins rising until reaching a "height of hysteria." After this high-water mark of public concern, public fears begin subsiding throughout the *deflating-fears* stage. Once a "point of practicality" is reached—that is, the point at which the technology becomes commonplace, integrated into the public's daily life—the "moving on" commences, characterized by the dissipation of public concern and marking the end of the panic cycle. Regarding UASs, Castro and McQuinn argue that the current debate is in the rising-panic stage:

> Given the prevalence of privacy advocates in the [drone] debate, the use of privacy rhetoric by policymakers when they discuss the technology, and the frequency of commercial drone coverage by the media, this technology has moved into its Rising Panic stage. Indeed, a 2014 survey found that nearly three-fifths of U.S. adults have privacy concerns about drones, despite only 3 percent of respondents having actually operated one. The privacy fears coalescing around this technology will continue to build until the technology is integrated into society and commonsense legislation is crafted to mitigate actual harms while protecting innovation. (2015, 21)

It is particularly noteworthy that so many individuals have expressed privacy concerns over UASs despite very few having hands-on experience with them. This is a defining characteristic of this early phase of the privacy panic cycle and will likely recede once a critical mass of the public is in close and regular contact with UASs.

Regarding the actual acquisition of consumer data, irrespective of the technological means by which it occurs, consumers' actions tend to be highly mismatched with their revealed preferences. As Will Rinehart has argued, "[P]eople will often state a preference for privacy, and yet will be very willing to trade information for little to nothing. These harms seem to be relatively costless" (2016). Ben Wittes and Emma Kohse concur and argue that this privacy paradox—wherein individuals may tend to state a preference for highly guarded privacy protections but reveal much less concern about the issue through their actions—is quite common:

> [T]he many studies of consumer attitudes toward privacy show a real gap between people's stated attitudes and their behaviors. For example, researchers who compared participants' self-reported opinions about privacy with their behavior during an online shopping experience found no correlation between greater concern for privacy and likelihood of taking privacy-protecting actions. Participants who reported concerns about protecting their privacy online were no less willing to reveal "even highly personal

> information." In another study researchers found that people tended to declare that they would refuse to provide certain personal information to marketers, but did, in fact, reveal that information when asked two weeks later. What people say about privacy does not seem to match what they do—even with respect to disclosure of specific personal information. (2017, 6)

Wittes and Kohse go on to conclude that people, taken as a whole, tend to "prioritize privacy from those around them over privacy from the remote companies that collect data on us and, indeed, a preference for facilitating highly local privacy at the expense of privacy from remote data-collectors" (2017, 16). Although Wittes and Kohse specifically examine competing privacy expectations in the online realm, these findings have implications specific to commercial UAS operations.

Despite varied consumer preferences regarding privacy, or perhaps because of it, the United States has a wealth of existing rules and regulations governing privacy at both the federal and the state levels.

Privacy Governance at the Federal Level

The United States, unlike many other countries, does not have baseline federal privacy rules. Privacy governance at the federal level instead tends to consist of, as Margot Kaminski describes them, "a series of sectoral regulations, enacted somewhat haphazardly. One federal statute governs privacy in video watching, one governs drivers' license information, one governs health information, one governs financial privacy, and so on. Drone-specific regulation would add to this patchwork" (2013, 65). Examples of these "sectoral regulations" include statutes such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Children's Online Privacy Protection Act (COPPA) of 2000, which regulate the use and disclosure of patient health-care information and online collection of information about children, respectively.

If one were pressed to identify the closest institution that serves as the domestic "privacy regulator" at the federal level, it would undoubtedly be the Federal Trade Commission (FTC). However, the FTC does not have a clear statutory authority to police privacy; it instead is imbued with the authority to police "unfair and deceptive practices" under 15 U.S.C. §45(a)(1)—the basic consumer-protection statute commonly referenced as Section 5. This statute permits the FTC to hold corporations accountable to the privacy promises made to consumers under user agreements, terms of use, and privacy-policy guidelines issued by corporations. As a result of this broad authority, the FTC, as Daniel Solove and Woodrow Hartzog have noted, possesses "a sprawling jurisdiction to enforce privacy in addition to the pockets of statutory jurisdiction Congress has given to it in industry-specific privacy legislation. The FTC reigns over more territory than any other agency that deals with privacy. Because so many

companies fall outside of specific sectoral privacy laws, the FTC is in many cases the primary source of regulation. FTC regulation is thus the largest and arguably the most important component of the U.S. privacy regulatory system" (2014, 588).

However, the agency currently lacks a clear, articulable framework for determining what precisely constitutes a privacy harm. To help remedy this knowledge gap, Castro and McQuinn recently proposed a typology of personally identifiable information (PII) to better guide the FTC's approach to considering resulting harms:

1. Observable information includes information that can be discerned by other individuals through firsthand observation (such as photographs or audio recordings).
2. Observed information is information about an individual that is drawn from third-party observation but cannot be used by another individual to reproduce the observation (such as date of birth or geolocation data).
3. Computed information refers to information that is produced from observed or observable information (such as online advertising profiles or credit scores).
4. Associated information is that which provides no descriptive information about an individual (such as driver's licenses or IP addresses). (summarizing Castro and McQuinn 2017, 2–4)

Using this framework, Castro and McQuinn go on to propose three types of "informational injuries" associated with each type of PII:

1. Autonomy violations are the result of private information becoming public via involuntary means.
2. Discrimination results from personal information being used to deny an individual access to a good or service.
3. Economic harms result from the misuse of an individual's information that causes financial damage. (summarizing Castro and McQuinn 2017, 5–6)

The type of informational injury an individual might experience is tied to particular types of information. Misuse of observable information can result in autonomy violations; misuse of observed information can result in either autonomy violations or discrimination; computed information could be misused for discriminatory harms; and associated information can result in economic harms (Castro and McQuinn 2017, 7). In the context of commercial UAS operations, the information type most directly relevant to potential injury would likely be observable information. Depending on the purposes for which the data are collected, however, harms could theoretically materialize from observed and computed information as well.

In addition to the FTC, federal legislation has also been proposed to address the privacy issues associated specifically with commercial UASs. The Federal Aviation Administration (FAA) Reauthorization Act of 2017 is the most notable such bill that

attempts to address these privacy concerns. It devotes an entire section to UAS considerations under Title II, Subtitle A ("Unmanned Aircraft Systems Reform"), and specifically touches on privacy in the following five provisions:

- Section 2101 would establish as an official policy of the United States that UAS operations "shall be carried out in a manner that respects and protects personal privacy consistent with the United States Constitution and Federal, State, and local law." (Hagemann 2017, 1)
- Section 2102 establishes that commercial UAS operators should have written privacy policies that are available publicly, updated regularly, and "appropriate to the nature and scope of the activities regarding the collection, use, retention, dissemination, and deletion of any data collected during the operation of [a UAS]." (Hagemann 2017, 1)
- Section 2103 directs the FTC to address privacy violations resulting from UASs operating "in the furtherance of a business enterprise." This is not a grant of new authority because the bill recognizes the FTC is already well situated to deal with potential harms under its Section 5 authority to police "unfair and deceptive" practices. (Hagemann 2017, 2)
- Section 2104 directs the FAA to create a searchable database of individual UAS owners as well as information pertaining to the circumstances under which a UAS is operated, where that UAS is operated, and the type(s) of information collected. Notably exempted from this database are news-gathering organizations protected under the First Amendment. (Hagemann 2017, 2)
- Section 2105 directs the comptroller general to produce a report that identifies those specific local, state, and federal laws "that address an individual's privacy" and identifies gaps in remedying potential privacy violations that result from the operation of UASs. (Hagemann 2017, 2)

These sections hint at the difficulty associated with crafting a one-size-fits-all approach to resolving the competing interpretations and applications of state and local privacy laws and federal rules governing commercial UAS operations. However, the FAA Reauthorization Act's focus on the FTC's Section 5 authority and the patchwork of state privacy statutes correctly identifies the major privacy pressure points that are likely to implicate future commercial UAS operations.

A Patchwork of State Laws

It has long been the case that the states, not the federal government, serve as "the historical locus of governance of personal privacy" (Kaminski 2013, 66). From California to Wisconsin to New Jersey, recent years have seen a proliferation of local ordinances and state legislation that attempt to craft penalties for UAS-specific privacy

violations and limitations on the technology's use. Cataloging these many proposed and enacted rules is beyond the scope of this paper. However, it is worth pointing out that these existing and proposed statutes as well as long-standing common-law decisions regarding privacy violations by private actors have largely served to effectively balance innovation and expectations of individuals' privacy protections.

The next section examines how some of these protections, such as privacy torts and the FTC's Section 5 authority, are robust enough to tackle any privacy issues that may emerge in the context of commercial UAS operations.

The Complex Intersection of Privacy and UAS Technology

The FAA has served as the safety regulator for the national airspace for more than half a century. However, the agency has no authority to establish privacy rules governing aerial surveillance. As a result, in 2015 the Obama administration directed the National Telecommunications and Information Administration (NTIA) to convene a multistakeholder process to develop nonbinding privacy best practices for UAS operators. The resulting document, *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability* (U.S. NTIA 2016), was released in May 2016. However, the voluntary, nonbinding nature of the promulgated standards do not carry the force of law, and whether a company chooses to abide by the best practices is unenforceable.

Such results showcase the difficulties in attempting to establish clear, binding, articulable, and practical rules governing privacy protections for commercial UAS operations. Indeed, these difficulties are further compounded by a lack of clarity surrounding what constitutes zones of "navigable airspace" in which UASs are permitted to operate.

Under 49 U.S.C. § 40102(a)(32), "navigable airspace" is defined as the "airspace above the minimal altitudes of flight prescribed by regulations under this subpart and subpart III of this part, including airspace needed to ensure safety in the takeoff and landing of aircraft." However, those subparts only add to the confusion because they offer no specific definition of the term *navigable airspace*. John Villasenor makes this uncertainty abundantly clear, noting that "[a]ttempts to identify a precise boundary where the 'immediate reaches' under the 'exclusive control' of a landowner end and the area available to the public begins can lead to complex questions" (2013, 491). Indeed, as Villasenor points out, the complexities are so pronounced that "the FAA can and does promulgate regulations that control the air all the way down to the ground, even over private property" (2013, 491).

This issue is directly relevant to UAS privacy considerations because potential violations of privacy by nongovernmental aerial operators will likely be implicated, in part, by the altitude of a UAS's flight. If an operator flies a UAS at one hundred feet above a private residence, is he violating residential airspace? What about eighty feet? Or two hundred feet? If a UAS is flying above the airspace "property" of a homeowner

but can still observe the homeowner in his secluded backyard, has an intrusion occurred? If the UAS is flying in publicly navigable airspace but can nonetheless intrude upon the seclusion of an individual, is that a privacy violation? What if the individual is not the object of the UAS's information acquisition, but his likeness is incidentally collected?

These questions are difficult, but even without baseline federal privacy regulations there are a host of legal mechanisms by which individuals can respond to such concerns. As Kaminski notes, "State privacy torts . . . cover what most people think of when they think of personal privacy and social privacy norms. . . . State privacy torts thus enforce social notions of personal privacy" (2013, 65). These privacy torts are most likely to address the more difficult questions surrounding commercial UAS data collection.

"With respect to civil liability," Villasenor notes, "courts in most jurisdictions recognize the two forms of common law invasion of privacy most likely to arise in connection with UAS: intrusion upon seclusion and public disclosure of private facts" (2013, 501). Intrusion upon seclusion and public disclosure of private facts are two of the four privacy torts originally detailed by William Prosser in his seminal law review article "Privacy," published in 1960. Prosser argued that "[t]he law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff, which are tied together by the common name, but otherwise have almost nothing in common except that each represents an interference with the right of the plaintiff, in the phrase coined by Judge Cooley, 'to be let alone'" (389). Those four torts are: (1) intrusion upon seclusion, (2) public disclosure of private facts, (3) publicity in a false light brought to the public eye, and (4) appropriation of name or likeness.

As previously indicated, interpretations of privacy differ by state and locality. However, in general, "to prevail in a common law or statutory intrusion upon seclusion claim, a plaintiff generally must establish, at a minimum, that the intrusion was intentional and that it would be 'highly offensive to a reasonable person'" (Villasenor 2013, 503). Whether the use of a nongovernmental UAS for commercial surveillance or data collection would qualify as "highly offensive" is unclear.

Although Villasenor notes the potential for the "public disclosure of private facts" tort to apply to UAS operations, much of his analysis is provided in the context of news-gathering and First Amendment considerations. Such concerns, though clearly present in the use of UAS technology, are slightly beyond the scope of this paper. Rather, the focus here is on the potential for more traditional commercial activities to result in privacy violations, such as data collection of publicly available information that is used to fuel innovative new products and services. To that end, contra Villasenor's focus on "intrusion upon seclusion" and "public disclosure of private facts," the primary privacy torts regarding non-news-gathering commercial UAS operations are more likely "intrusion upon seclusion" or "appropriation of name or likeness."

With respect to the difficult case scenarios of potential privacy violations, a Congressional Research Service report addressed many of these issues in 2015. It argued that

> [u]nder current law, the location of the target of the surveillance largely controls whether someone has a viable claim for both intrusion upon seclusion and publicity given to private life, and this is likely to hold true with drone surveillance. For the most part, using a drone to peer inside the home of another—whether looking through a window or utilizing extra-sensory technology such as thermal imaging—would likely satisfy the intrusion tort, and if photographs were taken and subsequently published, that person would also likely have a claim for publicity given to private life. (Thompson 2015, 16)

But are the privacy concerns regarding commercial UAS operations unique to the technological platform? Kaminski argues, in part, that they are:

> Drones do differ from existing surveillance technology in important ways, not because of one particular feature but because of an accretion of distinguishing features. But many of these features apply equally to camera phone use, or the use of remote biometric identification by private companies. Because of their relatively low cost and hovering abilities, drones give rise to a specter of pervasive surveillance, much like existing technology that can be used for surveillance, like camera phones. However, unlike surveillance by camera phone or most forms of CCTV, drone surveillance might provide no visible notice to the watched party. Unlike online surveillance, where, given notice, users at least can decide which sites to visit and which services to employ, drone surveillance gives no agency to the watched party. (2013, 72)

The issue of "notice" is particularly notable in the context of commercial UAS operations. However, Kaminski's points go beyond the nature of the UAS as a technological platform. It is not the UAS's actual flight operation that is at issue but rather the acquisition of data about individuals that may implicate privacy concerns. Remedying these potential privacy invasions requires an understanding of how collected data are treated and whether rules are better focused on acquiring preemptive permission from individuals or restricting the purposes for which collected data are used.

"Notice and Consent" versus "Limitations on Use"

Requiring consent before collecting information for use in a non–law enforcement context speaks to the broader—and ongoing—debate over data collection in the digital age. The rules for commercial data collection have long been governed by a regime of "notice and consent"—that is, service providers give *notice* of their intended use of collected data, and consumers *consent* by, in many cases, affirmatively agreeing to terms

of use or privacy policies before they can use the offered service. This debate is especially salient in the context of aerial data collection by private firms.

The previously referenced Congressional Research Service report aptly identifies the major fault lines regarding each of these privacy-governance approaches toward commercial UAS operations. Notice and consent, for example, may be unworkable in balancing privacy concerns with innovation because "[r]equiring consent before conducting aerial surveillance could undermine many uses of this new technology, making this theory of privacy [the right to control information about oneself] as applied to drone surveillance unworkable" (Thompson 2015, 7). Limiting the use of collected data may instead be a better avenue for addressing potential privacy harms; it has the benefit of disincentivizing policy makers from embracing front-end prohibitions on data collection. In addition, focusing on authorized or unauthorized uses of data would permit regulatory authorities, such as the FTC, to address harms based on existing grants of authority instead of necessitating the development of new regulatory powers. As the report points out, "[T]he initial collection may not directly implicate an individual's privacy interests, but the subsequent manipulation and storage of that data may warrant an alternative privacy analysis" (Thompson 2015, 9).

Although this solution to the privacy dilemma presented by commercial UASs may seem less than ideal, the reality is that data collection has become an inescapable, everyday part of life in the digital age. Craig Mundie, writing in *Foreign Affairs,* sums up this modern reality:

> Today, the widespread and perpetual collection and storage of personal data have become practically inevitable. Every day, people knowingly provide enormous amounts of data to a wide array of organizations, including government agencies, Internet service providers, telecommunications companies, and financial firms. Such organizations—and many other kinds, as well—also obtain massive quantities of data through "passive" collection, when people provide data in the act of doing something else: for example, by simply moving from one place to another while carrying a GPS-enabled cell phone. Indeed, there is hardly any part of one's life that does not emit some sort of "data exhaust" as a byproduct. And it has become virtually impossible for someone to know exactly how much of his data is [*sic*] out there or where it is [*sic*] stored. Meanwhile, ever more powerful processors and servers have made it possible to analyze all this [*sic*] data and to generate new insights and inferences about individual preferences and behavior. (2014, 28)

This reality is increasingly limiting the effectiveness of the traditional notice-and-consent regime. "It would be impossible," Mundie continues, "to write all the rules in advance or to craft a law that would cover every class of data and every potential use. Nor would it be sensible to ask people to take a few hours and write down how they might feel about any current or theoretical future use of their information" (2014, 34).

He advocates instead for placing limits on the use of collected information. This approach "would allow people to take firmer control of the information they care about by extending individual agency beyond the simple act of consent and permitting people to adapt their preferences and even rescind their consent over time" (34).

Commercial UASs pose a difficult challenge for would-be regulators, especially in an age when our social norms are constantly being reshaped by an endless and unceasing deluge of digital data. Ubiquitous interconnectivity poses a challenge not just for informal privacy norms but also for the legal boundaries and limits of our "right to be left alone."

The Impacts of Privacy Law on Commercial UAS Operations

Ultimately, a commercial UAS is a technological platform; what happens with the data after collection is not a concern specific to the mode of collection. Whether data are collected and improperly used ex post is an issue that is generally viewed apart from the means by which the data are acquired. Harms, if they materialize, can be remedied through existing regulatory authorities (such as the FTC), laws protecting specific types of information (such as HIPAA or COPPA), or common-law privacy torts. But the *type of data* that is collected is relevant in determining those potential harms.

Generally speaking, there are four primary types of drone-related data that could foreseeably be acquired for commercial purposes: (1) aerial video and photography, (2) thermal and infrared imaging, (3) geographic information mapping, and (4) three-dimensional modeling. Each *type of data* will invariably have an impact on the *type of harm* that may materialize as the result of publicly available information being collected by a commercial UAS operation. According to the Castro–McQuinn taxonomy, the type of PII likely to be implicated in UAS data collection would most likely be *observable information*. The information injuries likely to result from such collection would thus likely be *autonomy violations.*

Of course, all this is highly context dependent. A delivery or transportation UAS, for example, may be calibrated to acquire only the environmental data necessary to track its flight path. A UAS operated for infrastructure surveillance or pipeline inspections, by contrast, may require thermal imaging to fulfill its mission. Different types of data will necessarily implicate different potential harms, though the geographic area of operation will also matter, adding to the complexities of determining when or if a violation of privacy has occurred. A delivery UAS is less likely to require PII to fulfill its mission, but because it will most often operate in urban environments with high population densities, the likelihood of inadvertently acquiring PII increases (though it is unclear whether even inadvertently acquiring PII in such a context matters, given that such information would be obtained from a public forum). Alternatively, a UAS using thermal imaging to detect cracks in pipelines may be more likely to inadvertently acquire sensitive PII (such as radiative heat signatures from inside a home), but because its

operations are in more rural and remote areas, the lower population density means the privacy concerns may be significantly mitigated.

But what about a situation in which a commercial UAS is operated on a sustained basis, perhaps as part of a network of drones that are acquiring data to feed into a smart-phone app that provides real-time traffic (both sidewalk and road congestion) updates? Such a commercial service is unlikely to offer consumers significant value if it presents individuals with the opportunity to "opt-out" of its surveillance, given that its value is predicated on acquiring and documenting the presence (and direction and speed of movement) of individuals in a public space. And if the data are acquired from a public forum (that is, people walking and driving outside their homes, where expectations of privacy are significantly diminished), can individuals maintain that they have a reasonable expectation of privacy from aerial surveillance used for non–law enforcement purposes? Is the commercial UAS operator obliged to provide such an opt-out?

As with many of the other questions presented in this paper, the answer to this question is: it depends. Disclosure laws for data collection differ by locality, but many companies tend to provide both privacy policies and the ability to opt out of such collection as a cautionary approach to navigating evolving and uncertain privacy rules. This approach may change in the future, however.

On the one hand, if the FTC takes account of "the growing evidence about how consumers form their expectations, then it could increasingly demand that companies engage in practices that will correct mistaken consumer assumptions, or at the very least not exploit such assumptions. Existing forms of notice might not be deemed sufficient because the empirical evidence shows that consumers are not really being notified" (Solove and Hartzog 2014, 667). Alternatively, existing notice-and-consent regimes may be insufficient not because "the empirical evidence shows that consumers are not really being notified" but because it shows that consumers presume collection is occurring and, as Mundie previously suggested, have come to accept the new baseline expectations.

Conclusion

As Villasenor points out, "The only certain aspect of the debate about unmanned aircraft and privacy is that it will be contentious" (2013, 516). He concludes that the "near impossibility of predicting all of the ways that a rapidly developing technology can be used" is true for UASs just as it was true for the Internet in its early days:

> If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has

> created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later. (517)

A better approach, as Castro and McQuinn argue, would be to "pursue laws and regulations that uphold general expectations of privacy and mitigate against demonstrated privacy harms in the use of observable and observed information" (2017, 8). However, they caution, policy makers should also be aware "that cultural norms and standards over what to make public may change over time, and create regulatory flexibility to allow the market to adjust to changing expectations" (8).

The common law, too, will naturally develop baseline standards and statutory interpretations that reflect changing sociocultural norms in the context of UAS operations. Solove and Hartzog recognize this reality, noting that "[t]he common law is designed to develop gradually, and it often looks to societal norms when composing a standard. Indeed, in many other areas of law, as industry standards develop, failure to adhere to them makes it increasingly likely that those failing to adhere to them will be deemed negligent" (2014, 662).

Broader privacy concerns associated with data misuse are not unique to commercial UASs. Indeed, rules addressing observable harms to consumers are and ought to remain technology neutral. What those rules look like will be the result of consumer acclimation to this new technology, premised on a downturn in the rising panic of the privacy panic cycle, and of emerging consumer expectations surrounding the trade-off between privacy and innovation. As UAS operations increasingly become a common part of American life, regulators will adjust their approaches to adjudicating information injuries, and the common law will come to reflect changing social norms and privacy expectations.

For now, however, the future of commercial UAS operations and privacy laws remains up in the air.

References

Castro, Daniel, and Alan McQuinn. 2015. *The Privacy Panic Cycle: A Guide to Public Fears about New Technologies*. Washington, D.C.: Information Technology and Innovation Foundation.

———. 2017. *Comments to the Federal Trade Commission. RE: Informational Injury Workshop, Project No. 175413*. Washington, D.C.: Information Technology and Innovation Foundation.

Hagemann, Ryan. 2016. How We Think about Privacy Matters. Niskanen Center, June 16. At https://niskanencenter.org/blog/think-privacy-matters/.

———. 2017. Federal Aviation Administration Reauthorization Act of 2017 Title II, Subtitle A—Unmanned Aircraft Systems Reform. Niskanen Center, June 27. At https://niskanencenter.org/wp-content/uploads/2017/06/FAAReauthorizationActLegislativeAnalysis.pdf.

Kaminski, Margot. 2013. Drone Federalism: Civilian Drones and the Things They Carry. *California Law Review Circuit* 57, no. 4: 57–74.

Mundie, Craig. 2014. Privacy Pragmatism. *Foreign Affairs* 93, no. 2: 28–38. At http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism.

Prosser, William L. 1960. Privacy. *California Law Review* 48, no. 3: 383–423.

Rinehart, William. 2016. What Exactly Constitutes a Privacy Harm? American Action Forum, June 1. At https://www.americanactionforum.org/insight/exactly-constitutes-privacy-harm/.

Solove, Daniel J., and Woodrow Hartzog. 2014. The FTC and the New Common Law of Privacy. *Columbia Law Review* 114:583–676.

Thompson, Richard M. 2015. *Domestic Drones and Privacy: A Primer*. R43965. Washington, D.C.: Congressional Research Service.

U.S. National Telecommunications and Information Administration (NTIA). 2016. *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*. Washington, D.C.: NTIA, May 18. At https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf.

Villasenor, John. 2013. Observations from Above: Unmanned Aircraft Systems and Privacy. *Harvard Journal of Law and Public Policy* 36, no. 2: 457–517.

Warren, Samuel, and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4, no. 5: 193–220.

White House, Office of the Press Secretary. 2017. Presidential Memorandum for the Secretary of Transportation, Subject: Unmanned Aircraft Systems Integration Pilot Program. October 25. At https://www.whitehouse.gov/the-press-office/2017/10/25/presidential-memorandum-secretary-transportation.

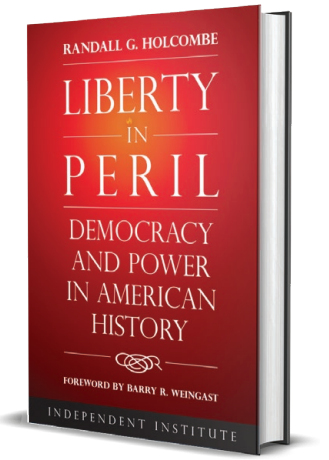
Wittes, Benjamin, and Emma Kohse. 2017. *The Privacy Paradox II: Measuring the Privacy Benefits of Privacy Threats*. Washington, D.C.: Brookings Institution, Center for Technology Innovation.

SUBSCRIBE NOW AND RECEIVE A FREE BOOK!

"***The Independent Review*** does not accept pronouncements of government officials nor the conventional wisdom at face value."
—**JOHN R. MACARTHUR**, Publisher, *Harper's*

"***The Independent Review*** is excellent."
—**GARY BECKER**, Nobel Laureate in Economic Sciences

Subscribe to ***The Independent Review*** and receive a free book of your choice such as ***Liberty in Peril: Democracy and Power in American History***, by Randall G. Holcombe.



Thought-provoking and educational, ***The Independent Review*** is blazing the way toward informed debate. This quarterly journal offers leading-edge insights on today's most critical issues in economics, healthcare, education, the environment, energy, defense, law, history, political science, philosophy, and sociology.

Student? Educator? Journalist? Business or civic leader? Engaged citizen? This journal is for YOU!

Order today for more *FREE* book options

SUBSCRIBE

The Independent Review is now available digitally on mobile devices and tablets via the Apple/Android App Stores and Magzter. Subscriptions and single issues start at $2.99. **Learn More.**

Download on the App Store | GET IT ON Google Play | Available on MAGZTER

INDEPENDENT INSTITUTE, 100 SWAN WAY, OAKLAND, CA 94621 • 1 (800) 927-8733 • ORDERS@INDEPENDENT.ORG