We tend to think of drones—or, more properly, “unmanned aerial vehicles” or “UAVs”—as a new phenomenon. However, the concept of using pilotless aircraft for military purposes has been around since at least the American Civil War period. Civilians have also used UAVs for recreation since remote controlled model aircraft were invented. Some of the problems with civilian UAV use also date back to those early days, including the risk of collision with people or property and interference with other aircraft or vehicles.

However, modern computing power and connectivity have changed both the functionality and the capabilities of drones. This article deals with one of those new risks: the potential for onboard video and audio to intrude on personal privacy.

Aerial photography has always had some capacity to affect privacy, and the prevalence of cell phone cameras as well as CCTV systems means that our images are being captured and potentially republished more than ever before. However, the use of drones, coupled with easy access to publication channels such as social media, create particularly intense new challenges. Current drone regulations in the US provide little in the way of explicit privacy protection. While the National Telecommunications and Information Administration (NTIA) has produced “best practices” to guide users about how to manage drones in a privacy-protective way, this framework does not have the force of regulation (https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf). There are also practical and conceptual difficulties with how some aspects of those guidelines apply to the drone environment.

A Brief History of Drones

UAVs—broadly defined as aircraft without a pilot—have an extensive history beyond what individuals have seen in headlines or their local store today. This technology has significant roots in military use before being adopted by civilians and emergency services.

Military Developments

UAVs—broadly defined as aircraft without a pilot—have a long history of development dating back to the Civil War. When UAVs were first conceptualized, they essentially consisted of loading up balloons with explosives, and users hoped that they would land on their intended targets. Precision was impossible. Missile
technology had improved significantly by World War II, but unmanned aircrafts were still in their infancy. For example, the Japanese launched balloons carrying explosives with the theory that air currents would carry the balloons to a target. This was labeled a failure.1

The US experimented with UAVs in WWII as well, but instead of using balloons they used planes. The plane was loaded with enough explosives to essentially make it a bomb. Pilots would fly the plane to a certain point, where (everyone hoped) they would bail out safely, and then a nearby aircraft would control the unmanned plane via radio control to its target. This was known as Operation Aphrodite, and had mixed rates of success.1 This approach, though, is much closer to how UAVs operate today, with someone controlling the aircraft via remote without actually having to set foot in a cockpit.

Since the 1940s, UAVs continued to be developed by the military and have been used in multiple wars for reconnaissance missions; photography and video were integral to their operation, including surveillance of people and their movements. UAVs gained the capability of carrying weapons only around 2002 during the war in Afghanistan. It is not coincidental that around this time the budget for UAVs increased significantly with one billion dollars allocated in the US budget for 2003.2

Civilian and Emergency Service Developments

From their origins in the 1930s, remote controlled model aircraft rapidly became popular, including being a perennial item on Christmas present lists for both children and adults. Specialized competitions and clubs sprang up. Instructors were available to help novice pilots learn to fly their increasingly sophisticated vehicles and avoid hazards. Recent technological developments and decreasing costs of basic drones have expanded the civilian market enormously. This includes the development of commercial applications for drone use, including agriculture, oil/gas, media, real estate, and filmmaking.3 Drones also have increasing value for emergency services where they enable close view without putting people at risk, for instance in police search and rescue operations in inaccessible regions, bushfires, and assessment of unstable buildings or accident sites. As of August 2016, there were roughly 20,000 drones registered with the Federal Aviation Administration (FAA) for commercial purposes. This number is expected to grow to nearly 600,000 after a change in FAA regulations made it easier for someone to be certified to pilot a drone.3 In 2016, drone sales for private use grew to $200 million, with models equipped with cameras and global positioning systems (GPS) dominating the market.4 However, regulation of drone use has been slower to develop than the market and is still arguably playing catch-up. For instance, in the US Congress passed legislation in 2012 directing the FAA to draft rules governing the use of commercial drones by 2015. Similarly, in New Zealand, the Civil Aviation Authority did not pass rules relating to drone use (or “remote piloted aircraft” as it formally calls them) until late in 2015.

Privacy Implications

The proliferation of drone use over the past few years has significantly increased the privacy concerns related to their deployment. Most of this is because drone capabilities have increased over the years to allow for sophisticated surveillance and data collection. The issues include the following:

- The majority of drones are equipped with— or designed to carry— cameras that both record pictures and video and are capable of storing and transmitting this information either immediately or for later viewing (typically through online upload). Some are also audio capable.
- The immediacy and normality of capturing and publishing information creates a significant need for user awareness of risks and a clear ethical framework within which to act. Taking privacy-invasive material down after the event is possible (though it may still persist in some form), but the damage may well have been done by then. However, the availability of drones has galloped ahead of clear guidance or agreed etiquette—let alone formal rules—on how to use them successfully.
- Drones are typically fairly small, especially when used by private citizens, with some capable of fitting in the palm of a hand. This allows them to be relatively invisible—that is, to enable covert surveillance—and to get into small places that a person cannot reach.
- Drones can also reach heights that are not accessible to other forms of commonly used modern devices such as the ubiquitous cell phone camera. They can therefore capture information that is well beyond what a normal cell phone user would be able to view: they are eyes in the sky.
- Another major factor in drone capabilities that creates additional privacy risks is their cost. Traditionally, surveillance of this type would be highly expensive, but drones today are inexpensive, with the average cost of those sold in the US in 2016 amounting to around $500.4 At this price, it is relatively easy for a large number of people to become model aircraft users, and it increases the likelihood of entry from commercial organizations.
- One effective method of protecting the privacy of an individual when collecting data is to ensure that there
are no personal identifiers within the data, either by ensuring one does not collect any personal data to begin with or by anonymizing the data (for instance by pixelation or blurring). However, it is unrealistic for the average personal user to engage such techniques. Even commercial entities may struggle. This form of advanced technology is relatively expensive and time consuming and would be less likely to be found on commercial or private drones. With the private use of drones, there is not a good mechanism to ensure that someone will take these privacy protection measures. Furthermore, at this point in time there are very few requirements for commercial companies to protect visual data in this way.

- While the law often does not extend to protect privacy in public places, because reasonable expectations of privacy are said to be limited, information captured by drones may well be different because they can capture what is not otherwise visible. Expectations of privacy can still be intact.

- Drones can capture images of people in their own homes: the place where we most obviously have a reasonable expectation of privacy. For instance, over the past few years, news outlets have reported several instances where drones have flown to someone’s window or over a private residence’s yard. Even the incursion of the aircraft is an intrusion, and when these drones are equipped with cameras, this is typically considered a privacy violation.

- It is difficult to know just from a visual inspection of the drone in flight if a camera is actually on and recording. Flying a drone over someone’s property cannot constitute trespassing according to a recent court case, though the law will differ from place to place. This makes it uncertain whether individuals can take action if they believe that someone is surveying them using a drone: proving what was recorded may be hard, and dealing with the incursion itself may also be legally problematic. As drones continue to have increasing technological capabilities, surveillance could be conducted far enough away from a property that the target could be completely unaware that he or she is being watched. While this is useful for law enforcement agencies, it is equally problematic when drones are available for private use. This opens the door to making certain types of criminal activity easier (for instance, stalking, peeping).

**Current Regulations for Drones in the US**

For reasons of space, this article considers only the US federal regulations for drones. However, regulations in other jurisdictions typically pick up similar themes and approach the issues in broadly similar ways. We recognize that many states have already passed their own drone regulation; however, much of this regulation overlaps with the FAA regulations discussed here, with few laws specifically focusing on privacy.

Regulations for drone use in the US are split in different ways. First, there are three categories of drone use: commercial, model aircraft, and military. The FAA is charged with regulating who can fly drones, pilot requirements, drone registration, and what airspace a drone is authorized to use for the two civilian groups (that is, commercial and model aircraft). The military tends to govern itself regarding the use of drones.

The FAA regulations for commercial use do not differ very much from model aircraft use. Some of the most noteworthy differences are related to the pilot requirements and the operating rules.

There is no pilot requirement for model aircraft use. However, to fly a drone for commercial purposes, a Remote Pilot Airman Certificate and Transportation Security Administration (TSA) vetting are required, and there is an age restriction (16). The ease with which someone might obtain a Remote Pilot Airman Certificate depends on whether they already possess another form of pilot license. The process is much easier if they do. However, for a first-time pilot, this certificate requires proficiency in the English language and the passing of an aeronautical skills test. This certificate expires after two years, at which point the pilot must take a refresher course to renew the certificate.

The operating rules for commercial and model aircraft uses are similar, but as with the pilot requirements, much more is explicitly stated for commercial use. The two FAA regulations that the commercial and model aircraft groups have in common are that the drone must be flown within the pilot’s line of sight and it must yield to any manned aircraft. Other than these two commonalities, it appears that commercial use of drones is regulated more heavily than model aircraft use. However, after examining the community safety guidelines that the FAA refers to for the model aircraft group, it becomes clear that this is not the case. The community safety guidelines include many of the regulations imposed on commercial drone use, including not flying over groups of people and/or events. In addition to these stipulations, the safety guidelines also include some rules that the commercial regulations do not explicitly state, such as recommending that pilots not fly under the influence and not fly near emergency situations. A summary of the regulations for commercial and model aircraft use can be found in Table 1.

**Privacy Best Practices (“Guidelines”)**

In addition to the regulations discussed earlier, the NTIA has also released a set of best practice guidelines in relation to privacy and drone use. They differ
from the regulations discussed above because they are merely recommendations for self-regulation and are not required by law. These guidelines specifically refer to practices related to data collected using drones, including transparency of data collection, methods of data collection, sharing, and storage of the data.

Like the FAA regulations for the use of drones, NTIA guidelines are separated into different sections: commercial, neighborly, and press. The press is included in addition to the first two categories in the best practices in order to carve out an exemption. Newspapers and news agencies, while commercial entities, are not asked to follow the guidelines because of the First Amendment protection regarding free speech and freedom of the press. These organizations typically have their own set of ethical guidelines, which the NTIA has referenced instead.

The first two categories of commercial and neighborly correspond with the categories (commercial and model aircraft) that the FAA previously defined in the drone regulations. As with those regulations, the best practices for commercial entities are more substantive than neighborly use. However, all drone operators, regardless of whether they are commercial or model aircraft, are advised to use the full set of guidelines whenever possible.

The major areas in the privacy guidelines are summarized in Table 2.

We discuss the main guidelines below.

**Transparency and Consent.** Informed consent is at the heart of the guidelines. A commercial entity that expects to collect data from individuals must inform them about the potential data collection and obtain consent for this data collection from the individual. Consent is defined as “words or conduct indicating permission.” This consent can be implied or explicit. As a general principle, this is of course good practice, though the specifics outlined in the guidelines decrease the power of this principle.

The method recommended for notifying individuals about data collection practices is through the posting of a privacy policy that outlines the purpose for which the data is collected, what the data will be used for, what kind of data will be collected, how this data will be shared and with whom, how to submit complaints, and how the entity responds to law enforcement requests (https://fpf.org/wp-content/uploads/2016/06/"UAS_Privacy_Best_Practices_6-21-16.pdf"). To some extent, this means transparency requirements (subject to the limitations below), but calling it “consent” is problematic.

First, privacy statements historically are not written with the best interest of the individual in mind, but with the purpose of protecting the company from litigation. They typically take the form of extremely lengthy documents and are written in high-level language. This results in very few individuals actually reading the documents. Assuming informed consent from an individual on the basis of a privacy policy alone is not going to be very effective in practice.

Second, and even more tellingly, there is the problem with where the privacy policy would be posted. Typically, when privacy policies are discussed, it is in reference to an online platform or terms and conditions about some technology. In-time communication is relatively easy in such circumstances: the privacy policy is easily accessible for use via a web link. For physical products, the seller can include a piece of paper with the technology. However, drones involve a third party using a particular technology to potentially collect information about others. While the guidelines do state that the entity should make reasonable efforts to notify individuals before the data collection takes place, they do not state that they should include their privacy policy in that notification. Even if one implies that they must, and even if that policy is publicly available, it does not mean it is easy to find or that it is reasonable and practicable for individuals to take the necessary steps to go and find it. Frankly, it is often impractical for drone users to

### Table 1. FAA civilian drone regulations.*

<table>
<thead>
<tr>
<th></th>
<th>Commercial</th>
<th>Model aircraft</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pilot requirements</strong></td>
<td>Must have passed TSA vetting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>Must have a Remote Pilot</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Airman Certificate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Must be over the age of 16</td>
<td></td>
</tr>
<tr>
<td><strong>UAV requirements</strong></td>
<td>Must be under 55 lbs, or be registered if over 0.55 lbs</td>
<td>Must be under 55 lbs, or be registered if over 0.55 lbs</td>
</tr>
<tr>
<td></td>
<td>Must undergo preflight check</td>
<td></td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td>G airspace</td>
<td>Five miles from an airport (without prior authorization)</td>
</tr>
<tr>
<td><strong>Operating rules</strong></td>
<td><strong>UAV must:</strong></td>
<td><strong>UAV must:</strong></td>
</tr>
<tr>
<td></td>
<td>~ Yield to any manned aircraft</td>
<td>~ Yield to any manned aircraft</td>
</tr>
<tr>
<td></td>
<td>~ Stay within line of sight</td>
<td>~ Stay within line of sight</td>
</tr>
<tr>
<td></td>
<td>~ Fly under 400 feet</td>
<td>~ Follow community-based safety</td>
</tr>
<tr>
<td></td>
<td>~ Fly at less or equal to 100 mph</td>
<td>guidelines</td>
</tr>
<tr>
<td></td>
<td>~ Not fly over people</td>
<td></td>
</tr>
<tr>
<td></td>
<td>~ Not fly from moving vehicle</td>
<td></td>
</tr>
</tbody>
</table>

*Table adapted from Federal Aviation Administration website: https://www.faa.gov/uas/getting_started.
inform people before or at the time of collection that the collection is occurring (the collection be incidental to the purpose of using the drone), and tracing the relevant individuals after the event to ask for consent may not always be possible.

The third problem lies with the notion of consent itself. Consent, as outlined in these guidelines, can be explicit or implied. If the entity makes a reasonable effort to notify individuals about data collection, it appears that the entity would be able to assume that no response from these individuals means that they consent. This is more commonly known as “opting out.”

When an individual opts in for a program, there is an assumption that unless the entity hears something from the individual, then the answer is “no.” Realistically, the nature of the activity and issues of timing mean that individuals are not likely to be given the choice to opt in, however preferable this might be from a privacy perspective.11

Transparency is an important privacy protection, but there are real questions about the practicality of making that information available and the validity of asking for consent in the drone environment. Relying on a privacy policy alone to establish implied consent is conceptually problematic. However, creating mechanisms to obtain consent is useful and worthwhile if the drone use is a planned activity (such as filming a sporting event) where it is obvious that information about individuals will be captured and particularly where the individuals may be the subjects of the footage.

When images of identifiable individuals are captured incidentally or accidentally as part of the drone activity, though, consent may be impracticable, and reliance on a privacy policy to provide consent does not work at all. Notice and choice are simply insufficient to protect privacy. Much greater emphasis needs to be placed on the other safeguards covered in the guidelines.

Table 2. Privacy best practice summary.

<table>
<thead>
<tr>
<th>Area of interest</th>
<th>Guidelines provided</th>
</tr>
</thead>
</table>
| Privacy policy   | Should be publicly posted  
|                  | Should contain information regarding:  
|                  | – The purpose for the data collection  
|                  | – Types of covered data collected  
|                  | – Data storage and anonymization practices  
|                  | – Procedures for submitting complaints/concerns  
|                  | – Responses to law enforcement requests  
| Data collection  | Operators should not:  
|                  | – Collect covered data where the individual has an expectation of privacy†  
|                  | – Continuously collect covered data of individuals‡  
| Data storage     | Operators should avoid retaining data longer than necessary†  
| Data security    | Operators should develop an information security policy from one of these known standards:  
|                  | – Federal Trade Commission  
|                  | – NIST Cybersecurity Framework  
|                  | – ISO 27001 standard for information security management  
| Data use         | Data should not be used for:  
|                  | – Employment eligibility, retention, or promotion†  
|                  | – Credit eligibility‡  
|                  | – Healthcare treatment eligibility‡  
|                  | – Any purpose not listed in the privacy policy  
|                  | – Marketing purposes‡  
| Data sharing     | Data should not be shared:  
|                  | – With anyone not listed in the privacy policy  
|                  | – Publicly‡  
|                  | – For marketing purposes‡  

* Unless there is a compelling reason to do otherwise.  
† Unless consent is obtained.  
‡ Table constructed from the National Telecommunications and Information Administration Privacy Best Practices for UAS.

When an individual opts in for a program, there is an assumption that unless the entity hears something from the individual, then the answer is “no.” Realistically, the nature of the activity and issues of timing mean that individuals are not likely to be given the choice to opt in, however preferable this might be from a privacy perspective.11

Transparency is an important privacy protection, but there are real questions about the practicality of making that information available and the validity of asking for consent in the drone environment. Relying on a privacy policy alone to establish implied consent is conceptually problematic. However, creating mechanisms to obtain consent is useful and worthwhile if the drone use is a planned activity (such as filming a sporting event) where it is obvious that information about individuals will be captured and particularly where the individuals may be the subjects of the footage.

When images of identifiable individuals are captured incidentally or accidentally as part of the drone activity, though, consent may be impracticable, and reliance on a privacy policy to provide consent does not work at all. Notice and choice are simply insufficient to protect privacy. Much greater emphasis needs to be placed on the other safeguards covered in the guidelines.

Covered data. The document is very specific about what types of data are “covered.” Covered data is any data that “identifies a particular person.” If the information cannot be linked to an individual’s name or any other personally identifiable information (PII), then it is not covered data. This is a significant departure from current privacy laws and policy where protected data is limited to specifically defined types of personally identifiable information. It goes beyond what is traditionally protected. In our view, it does this in a way that appears justified and necessary in the context.

Historically, in US law (though not in jurisdictions with broader privacy laws), protecting PII is closely related to protecting against identity theft. This means that the items included in the definition of PII are typically limited to name, Social Security number, driver’s license number, bank account numbers, and address. It does not include still or moving images or audio files, which are covered by the guidelines. At this time, multiple technologies exist that can identify an individual based on various attributes including voice and likeness (for example, image).12 This expanded definition of PII is necessary when discussing drones because the traditional forms of data collected by drones would not be covered by current definitions of protected data. The guidelines in this case provide more privacy protection than many laws (for example, the Telecommunications Act) today.
The guidelines cover only information that is capable of leading to an individual's identification. They state that information is not covered if it "likely will not be linked to an individual's name or any other personally identifiable information, or if the data is altered so that a specific person is not recognizable." However, it is well known that anonymization is not effective in protecting an individual's privacy: see for instance the studies on re-identifying individuals from combined datasets. Facial recognition technologies are improving significantly, including image recognition that can identify people out of photographs posted on social media. There are currently methods that can permanently obscure an image, but these require an extra step after data collection.5

It is foreseeable that many entities that apply the guidelines will underestimate the likelihood of individuals being identified, for instance, if they post the footage on social media (which is permitted only if necessary, as we pointed out earlier on the problems with consent and necessity above). It is common for agencies to look at such clauses through the lens of their own intentions, not to look at what is objectively possible in the context—that is, if the agency itself does not intend to identify those individuals, it may assume that the data is not covered by the guidelines. It may therefore be beneficial to expressly alert unmanned aerial system (UAS) operators to the need to take care when publishing images in situations that may allow others to identify individuals who are featured. This includes using images in advertising or posting them online.

**Data collection, storage, and sharing practices.** The remainder of the privacy guidelines focuses on the collection, storage, and sharing of covered data. In general, unless the operator of the drone has received the explicit consent of the individual or has a compelling reason, he or she should refrain from collecting data. The guidelines do not define the term "compelling reason" in order to give the practices more flexibility for different entities that would use them.

Using a strong term such as "compelling reason" is a useful signal that if consent is not possible, there must be a clearly justifiable reason for the collection. However, not defining this term hurts individuals who could be the subject of data collection because what they would define as a "compelling reason" will not always be the same definition of the operator. The decision to not define this term leaves far more room for interpretation than what is necessary for this document.

Instead, the guidelines could make it plain that a "compelling reason" will only exist where:

- the personal information is collected for a lawful purpose;
- the data collection with drones is genuinely relevant to what the agency does;
- the potential for an individual to suffer harm from a breach of their privacy is limited; and
- there is no realistic and less intrusive alternative to collecting this information in order to meet the agency’s aim—that is, the collection is effective and proportionate.

Drone operators should also avoid retaining collected data for an extended period of time. When the data is retained, there should also be efforts to keep this data secure. Specifically, the guidelines state that the entity should “implement a program [with] reasonable administrative, technical, and physical safe-guards appropriate to the operator's size and complexity, the nature and scope of its activities, and the sensitivity of the covered data.” This language is quite vague and bureaucratic. Both the words reasonable and appropriate are open to interpretation. What seems reasonable or appropriate to one operator may seem excessive to another. Because the guidelines never define either of these terms, there is no unified expectation for privacy protections.

The guidelines recognize the problem and have referred to several reputable organizations (that is, the Federal Trade Commission, NIST Cybersecurity Framework, and the ISO) that operators can use as resources to develop a good information security policy. Given that these are privacy best practices and not regulations, referencing these standards of information security is helpful. However, smaller drone operators may struggle to unpack what these external resources mean (particularly the NIST and ISO frameworks) and how they can apply the relevant points to their own situations. If the guidelines are to be observed, it is important to make life easier for small businesses and individuals who will use them. We suggest that the guidelines could distill the main points from the external guidance and communicate it clearly to users (perhaps in the form of a “top ten” list of things to check or implement).

The final area that the best practices discuss is about how data should be shared and used. While several other areas of the best practices are vague, they are more explicit in regards to how this data may be used. Specifically, data collected by drones cannot be used (without consent) to determine “employment eligibility, promotion, or retention; credit eligibility; health care treatment eligibility.” The exception to this is if it is permitted by another regulatory framework. This is a logical and necessary exception, but given the patchwork nature of US laws and regulations, finding out what other laws might apply is not always the easiest task in practice.
Apart from those specific areas, the operator should not use or share the information outside of circumstances specified in the privacy policy. Clearly, operators need to comply with what they have said they are going to do; to do otherwise would be misleading. The reference is therefore unobjectionable, and is possibly a useful reminder for the operator, but it does not provide any further privacy protection. As mentioned earlier, relying on a privacy policy for any type of consent is not in the best interest of the individual because of elevated language typically used and the likelihood of someone reading it is not great.8,10

As for the public release of the data collected, operators are advised to not do so unless necessary. If they are required to publicly release information, they should take steps to anonymize the data. As stated earlier, this is not a good measure of privacy protection.

Interaction between FAA Regulations and NTIA Best Practices

As briefly mentioned earlier, the privacy guidelines were released by the NTIA, not the FAA. This is because the FAA does not have the authority to regulate activities related to the collection and handling of data. Whether it can issue nonbinding guidance is perhaps moot: it does not appear that it considers the issuing of privacy guidance as part of its core role. Instead, this task falls to the NTIA, which released the guidelines after consulting with multiple stakeholders concerning the operation of drones.

The fact that two different agencies are regulating and advising on the topic has some implications for privacy in the use of drones. It is not necessarily obvious to operators (particularly model aircraft users, but even small business operators) where to look for the rules or advice. It may also not be obvious what the status of documents produced by each body may be. Confusion about what is a required rule and what is voluntary best practice is not helpful, and can raise risks of noncompliance or of risk aversion and excessive compliance costs. Even in the NTIA guidelines, there is some confusion. The only section of the privacy guidelines that directly refers to the FAA is section 2c, which states (emphasis ours):

Where it will not impede the purpose for which the UAS is used or conflict with FAA guidelines UAS operators should make a reasonable effort to minimize UAS operations over or within private property without consent of the property owner or without appropriate legal authority.

Yet, as we know, the FAA has imposed regulations on commercial and model aircraft operators—not guidelines. Those regulations have the force of law and must be followed, or the operator will suffer consequences. However, more positively, several of the FAA regulations reduce some of the concerns raised earlier about protections in the privacy best practices. First, the privacy guidelines state that the operator must have in place some way for individuals to file complaints or make requests that their data be deleted. There is a concern that it may not be easy for an individual to find this particular information. It should be in the privacy policy, but unless the individual knows who the drone operator is, this may be of little use. However, an FAA regulation offers a slight bit of help by requiring every drone over 0.55 lbs to be registered. If this registration information is publicly accessible, and one can visually identify the registration on the drone from a distance, then it would be possible for the individual to look up the operator from the registration. However, we note that this is a lot of “ifs”: the chances of everything lining up are not particularly high.

Second, the drone must always be within visual distance to the operator (without aided vision, for instance, binoculars, scope). Although this does not stop operators from hiding from those observed, it can provide more of an opportunity for individuals to confront them to file a complaint than if they were a few miles away from the drone. As we noted earlier, though, technological improvements make it possible to obtain clear images of individuals while the drone is a long way from the individual. The line of sight rule is important for safety, as it makes it more likely that the UAV will be flown competently, but it is less useful for privacy. The increasing number of near-misses between drones and piloted aircraft, and the difficulties that the authorities experience with tracking the drone operators responsible, make it plain that the ordinary individual faces an uphill struggle with identifying operators, finding out whether a privacy violation has occurred, and holding the operator to account if it has.

Policy Recommendations

The privacy guidelines released by NTIA follow in the tradition of US privacy policy in that there is an expectation of industry self-regulation. However, if the self-regulation platforms are any indication of what self-regulation looks like, it typically does very little to protect individuals. Research shows that industry self-regulation at this time has no impact on preventing data breaches. In addition, there has been a proven track record of noncompliance with companies registered with self-regulatory programs. However, there is no clear indication how this noncompliance is addressed.11 At the very least, the guidelines also need an amendment to enhance the privacy protection that they offer while also recognizing the significant benefits that drone technology provides for both commercial enterprises and model aircraft users.
The effectiveness of voluntary guidelines will always be limited, however, and it is important to eliminate the confusion that currently exists between what is law and what is optional. But the biggest weakness of self-regulation is the lack of an enforcement mechanism. Individuals have no guarantee that drone operators will follow industry best practices, and no clear action is specified if it is determined that these best practices have been violated. This concern has been echoed by both potential bystanders to drone operation and drone operators.\(^\text{15}\) We therefore believe that it is better for the US to adopt and enforce privacy regulation concerning the use of drones. The regulation should cover many of the matters in the guidelines, including development of accessible privacy policies, the need for consent where practicable, limits on when personal information can be collected (so that situations where consent is not possible are governed), limitations on use and disclosure, and rules about retention. Any privacy protection mechanism should consider the privacy of bystanders as well as drone operators because some potential methods for enforcement could impact the privacy of drone operators by subjecting them to data collection.\(^\text{15}\) Federal regulation is recommended to ensure that all individuals who reside in the US have a minimum standard of privacy protection and for the purposes of clarity for drone operators. As with other privacy regulation today, state legislators still have the option to enact stronger privacy protections as they deem necessary.

These recommendations are more in line with how European law deals with privacy but are still workable in the US context. Even so, there are potential barriers that could significantly impact the implementation of our policy recommendations. First, the political climate of the US makes it increasingly difficult to pass legislation at the federal level. Maintaining consistent regulation outside of legislation is just as difficult because many regulatory agencies are dependent on Presidential appointments for their positions. As can be seen with the Federal Communications Commission’s attempt to reverse the net neutrality policies introduced in 2014, regulation could shift depending on which party holds power within the regulatory agency. Second, harming innovation is frequently cited as a barrier to privacy protections. We recognize that our policy recommendations could potentially harm smaller drone operators. However, this is a potential harm with any regulation that is introduced. In this situation, we believe that that benefits outweigh the costs.

It is our view that appropriate and proportionate regulation of drone use to protect personal privacy is becoming critically important as drones continue to proliferate and their commercial and recreational uses become more varied. The pressure on airspace and the potential for intrusions into personal space are only going to grow greater.

UAVs represent a significant opportunity for developing new business processes and services, and it is important not to stifle innovation. However, the ability to innovate will be undermined if drones are operated in an untrustworthy manner. Considering regulation through a privacy lens as well as a safety lens enables us to gain the benefits from UAVs while avoiding the worst of their potential harms.

The current combination of the FAA regulations and NTIA guidelines do not go far enough to provide clarity and certainty for users or for the public who may be the subjects of either deliberate or accidental drone surveillance. More needs to be done in both fields, but it does not seem likely that anything short of regulation—where there are consequences for failure to comply—will be effective enough to drive safer and more trusted behavior in this fast-moving environment.

References


Stephanie Winkler is a PhD candidate at The Pennsylvania State University in Information Sciences and Technology. Her current research interests include privacy, security, human–computer interaction, and fake news and misinformation. She received a master’s in communication from the University of Kentucky. Contact her at sxw96@ist.psu.edu.

Sherali Zeadally is an associate professor in the College of Communication and Information at the University of Kentucky. His research interests include cybersecurity, the Internet of Things, privacy, and computer networks. Zeadally received a doctoral degree in computer science from the University of Buckingham, England. He’s a Fellow of the British Computer Society and the Institution of Engineering Technology, England. Contact him at szeadally@uky.edu.

Katrine Evans is a privacy lawyer in Wellington, New Zealand, and is currently a senior associate at Hayman Lawyers. Before going into private legal practice, Evans was Assistant Privacy Commissioner for more than a decade, including acting as the Commissioner’s general counsel and managing the policy and technology team. Contact her at k.evans@haymanlawyers.co.nz.