Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft

August 2, 2016

FUTURE OF PRIVACY FORUM

PRECISIONHAWK

intel

About The Future of Privacy Forum

The Future of Privacy Forum (FPF) is a Washington, DC, based think tank that seeks to advance responsible data practices. FPF includes an advisory board comprised of leading figures from industry, academia, law, and advocacy groups. More information about FPF can be found at www.fpf.org or on Twitter @futureofprivacy.

About Intel

Intel invents at the boundaries of technology to make amazing experiences possible for business and society, and for every person on Earth. Harnessing the capability of the cloud, the ubiquity of the Internet of Things, the latest advances in memory and programmable solutions, and the promise of always-on 5G connectivity, Intel is disrupting industries and solving global challenges. Leading on policy, diversity, inclusion, education and sustainability, Intel creates value for our stockholders, customers and society. More information about Intel can be found at www.intel.com or on Twitter @Intel.

About PrecisionHawk

PrecisionHawk is a terrestrial data acquisition and analysis company founded in 2010. The company provides an end-to-end solution using Unmanned Aerial Vehicles (UAVs) for data collection and analysis software tools to deliver better business intelligence to clients across a wide range of civilian industries. PrecisionHawk also owns terrestrial data software, DataMapper, satellite imagery provider, Terraserver, and the Low Altitude Traffic and Airspace Safety platform for drones, LATAS. More information about PrecisionHawk can be found at www.precisionhawk.com or on Twitter @PrecisionHawk.

Acknowledgements

Drones and Privacy by Design: Embedding Privacy Enhancing Technology in Unmanned Aircraft was written by FPF EU Fellow Laura Vivet and FPF Policy Counsel Lauren Smith. The report was produced in collaboration with Intel and PrecisionHawk.

TABLE OF CONTENTS

Introduction

Commercial drone operations are rapidly expanding and promise major benefits for society. Drones can save lives and support critical projects, including search and rescue missions, medicine delivery, precision agriculture, mapping, and aerial photography.

However, drone operations can result in collection, use, or sharing of personal information, including information about individuals who are not involved in the flights. Some consumers have concerns about drone data collection, and policymakers agree that responsible data practices are crucial to building trust in drone services.

The Future of Privacy Forum (FPF), Intel, and PrecisionHawk have long supported privacy enhancing technologies and advocated for "Privacy by Design" – a framework that embeds privacy safeguards into the design of IT architecture and business practices.[1] In 2013, FPF called on drone companies to use privacy by design principles to bolster trust in then-nascent commercial drone operations.[2] Since 2013, commercial drone flights have become increasingly common; the Federal Aviation Administration's recently promulgated Small UAS Rule promises to open the skies to even more drones.[3] In May 2016, a diverse group of leading stakeholders reached consensus on best practices to promote privacy, transparency, and accountability for commercial and recreational drone operation.[4] The best practices urge drone users to take reasonable, practical steps to safeguard personal data. Below, we discuss concrete examples of how drone manufacturers, operators, and others are employing privacy by design principles to help users respect privacy and promote trust in drone operations.

The Privacy-by-Design framework states that developers should embed privacy into the design and architecture of devices, systems and business practices. In doing so, privacy is enabled by default, not "bolted on as an add-on, after the fact."[5] Privacy-by-Design requires that developers ask questions about what data is collected, how it is used, with whom it is shared, how much of that data is retained, and how data is stored and protected. In doing so, they consider the benefits and risks of the use of data, and what steps can be taken to mitigate risk. For example, in some cases the privacy-by-

[1] "IPC - Office of the Information and Privacy Commissioner/Ontario | Introduction to PbD." IPC - Office of the Information and Privacy Commissioner/Ontario | Introduction to PbD., https://www.ipc.on.ca/english/Privacy/Introduction-to-PbD.

[2] Jerome, Joseph. "Domestic Drones Should Embrace Privacy by Design - Future of Privacy Forum." 2013, https://fpf.org/2013/04/05/domestic-drones-should-embrace-privacy-by-design/.

[3] "Press Release – DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems." Press Release – DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems. https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515.

[4] Bates, Melanie. "Multi-Stakeholder Group Finalizes Agreement on Best Practices for Drone Use - Future of Privacy Forum." Future of Privacy Forum. May 18, 2016, https://fpf.org/2016/05/18/14421/; *Voluntary Best Practices for UAS Privacy, Transparency, and Accountability*. NTIA, 2016, https://fpf.org/wp-content/uploads/2016/06/UAS_Privacy_Best_Practices_6-21-16.pdf.

[5] Cavoukian, Ann, Ph.D. Information & Privacy Commissioner, Ontario, Canada. *Privacy by Design: The 7 Foundational Principles*. Toronto, Ontario, 2011, available at https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

default decision is to choose to minimize data collection; in others it may be to enhance security for data that is processed and retained.

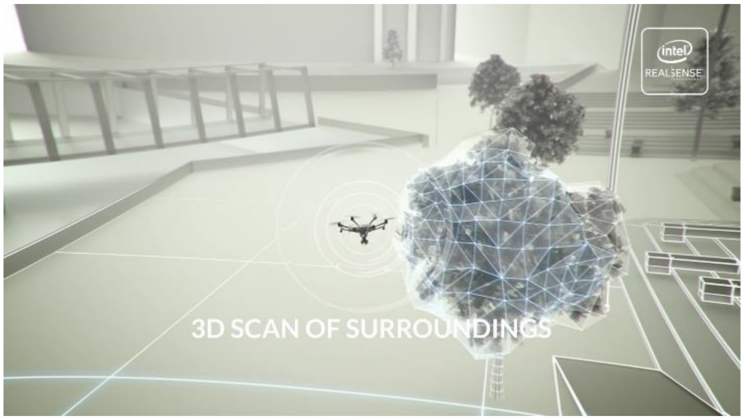
The examples discussed in this paper illustrate how Privacy-by-Design decisions about data collection can be integrated into the architecture of drone devices and the technologies that can make that possible.

1. Embedding Privacy by Design in Sense and Avoid Solutions

The Privacy by Design framework states that privacy ought to be embedded into the design and architecture of systems and business practices and enabled by default, not "bolted on as an add-on, after the fact."[6] This principle is embodied by leading crash avoidance software used by some drones.

Whether drones are piloted by humans or flying autonomously, they typically use "sense and avoid" technology – software that helps drones automatically detect objects and navigate around them safely. Sense and avoid systems typically rely on imaging technologies to map their physical environment. Some of this data is crucial to ensuring safe flight, but comprehensive collection and retention of image data could create privacy risks.

Intel's *RealSense* computer vision system, combined with sense and avoid software, is one technology that can help drones process images while only collecting the minimum data necessary for collision avoidance.[7] *RealSense* uses a combination of 3 sensors: a standard digital camera, an infrared camera, and an infrared laser projector.[8] These sensors, controlled by a drone-mounted computer, measure the depth of objects and map the world around the drone, automatically avoiding obstacles while in flight. Combined with GPS, altitude and other onboard sensors, the technology can also avoid no-fly areas.



Intel RealSense Video

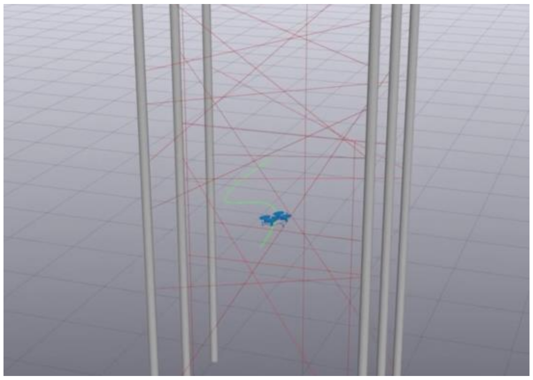
[6] *Id.* at 5.

[7] Kaplan, Ken. "New Era For Smart Drones That Can See." January 6, 2016. https://iq.intel.com/new-era-for-smart-drones-that-can-see/.

[8] "Intel® RealSense™ Technology." http://www.intel.com/content/www/us/en/architecture-and-technology/realsense-overview.html.

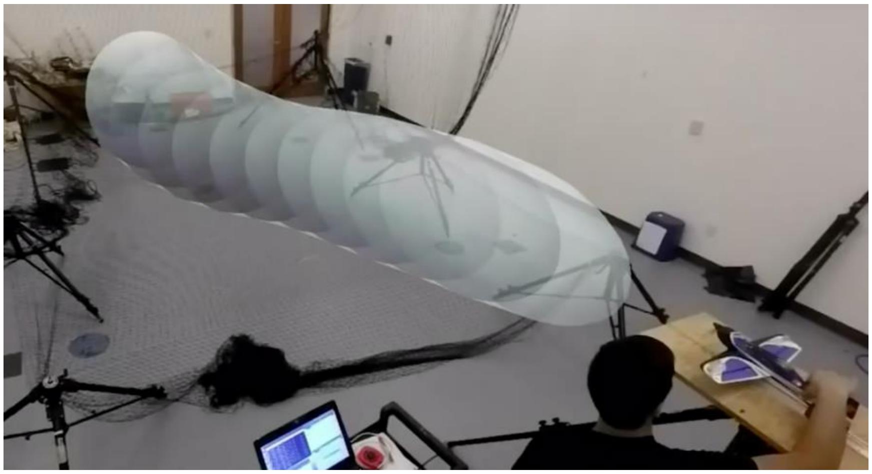
RealSense algorithms turn the imagery collected by drone cameras into data that is useful for avoiding hazards, but can discard much of the raw image data that could identify nearby people.

Additional technologies are under development that will improve drones' ability to sense and avoid dangerous locations while minimizing collection of personal data. One team of researchers from the MIT Computer Science and Artificial Intelligence Lab have demonstrated software that allows drones to avoid obstacles while in flight using algorithms to segment space into 'obstacle-free regions' and linking regions together to find a collision-free route while flying.[9] Rather than scan the nearby environment (including nearby people) to detect obstacles and avoid them, the software identifies known free-space segments between a drone operator's start point and destination, crafting a safe flight plan while minimizing collection of personal data.



MIT CSAIL Obstacle-Free Region Mockups

Another MIT research team developed software that allows drones to plot routes while avoiding obstacles by searching a library of distinct pre-computed funnels that represent the worst-case behavior of the system calculated via a verification algorithm. The drone then searches the library and stitches together a series of paths that are computationally guaranteed to avoid obstacles. [10]



MIT CSAIL Funnel Research

Drone sense and avoid systems rely on sensors to promote safe flight, but as described above, sense and avoid systems can be designed such that images are processed in real time and only safety-critical data is retained. These systems do not require retention of personal data to operate without retaining personal data.

[9] Conner-Simons, Adam. "Watch Drones Do Donuts around Obstacles Thanks to Planning Algorithms." MIT Computer Science and Artificial Intelligence Laboratory (CSAIL). January 19, 2016. http://www.csail.mit.edu/drones_do_donuts_around_obstacles.

[10] *Id; see also* Majumdar, Anirudha and Russ Tedrake. " Funnel Libraries for Real-Time Robust Feedback Motion Planning." Computer Science and Artificial Intelligence Lab, Massachusetts Institute of Technology, 2016. http://groups.csail.mit.edu/robotics-center/public_papers/Majumdar16.pdf.

2. Embedding Security by Design

Securing personal data is a key privacy safeguard, and leading drone companies enable security by design. Drones are flexible platforms that can carry a wide array of sensors and collect a wide range of data, including personal information. When drones collect and retain personally identifiable information, operators typically seek to secure the data stored on board the drone. This is particularly important because drones can be vulnerable to physical capture and malicious attacks through impersonation, manipulation and interception. When drones collect and transmit PII to the operator in real time, operators can employ secure communications protocols to reduce the chance personal data will be intercepted.

Leading drone manufacturers and operators employ a variety of techniques to secure data stored on drones and transmitted from unmanned aircraft.

The Association for Computing Machinery (ACM) has outlined an approach that can minimize information data leakage when drones are physically accessed by unauthorized individuals.[11] The approach uses an efficient cryptographic mechanism that takes into account the constrained computing resources of smart objects and the mobility and limited flight time of drones. It combines one-way key agreement and digital signatures into an efficient algorithm. The system uses partial private keys valid for a defined time period. After the time period expires, new private keys are generated. Accordingly, if a drone is captured, information leakage is limited to the time period during which the private keys were valid. This approach permits operators to set a time limit – roughly the expected time of the drone operation – after which the data is rendered inaccessible. If a drone crashes or is intercepted, time-limited keys reduce the opportunity for an unauthorized individual to access personal data collected by the drone.

3. Embedding Privacy in Drone Navigation Controls

3DR Solo Geo-Fencing

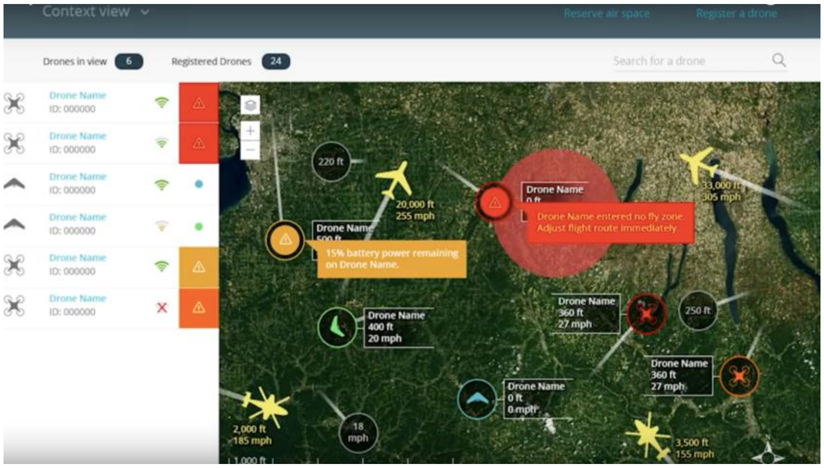
Collecting and retaining imagery requires significant processing and storage capabilities. Drone operators therefore have strong incentives to collect the most precise and useful data possible about the relevant area, and to avoid collecting data outside that area.

Operators routinely employ navigation controls (also called "airspace management services") to establish virtual geo-fences for drones, restricting

[11] Jongho Won, Seung-Hyun Seo and Wlisa Bertion, "A Secure Communication Protocol for Drones and Smart Objects", In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, (ASIA CCS '15). ACM, New York, NY, USA, 249-260. https://www.cs.purdue.edu/homes/won12/pub/[4]_ASIACCS2015_A%20Secure%20Communication%20Protocol%20for%20Drones%20and%20Smart%20Objects.pdf

flights to particular areas and preventing overbroad, unintended data collection that could capture personal data about individuals who are in adjacent areas. These practices help ensure that drone pilots or autonomous software fly in the intended area and collect little, if any, data outside the geo-fenced region. Navigation controls, which are available for nearly all drones, can preserve privacy by reducing unintended recording of individuals. The controls are also a key accountability mechanism, allowing operators to establish data collection policies and ensure pilot compliance.

Drone operators use several tools to prevent drones from capturing data away from the intended flight path; these tools help embed privacy in drones used by companies and hobbyists.



15% battery power remaining on Drone Name.

Drone Name entered no fly zone. Adjust flight route immediately.

LATAS Geo-Fencing

For example, PrecisionHawk, a partner in the FAA's Pathfinder Program and the NASA UTM Program, developed the LATAS Platform, which helps advance this goal.[12] LATAS uses cellular network and satellite infrastructure to track the position of each drone, analyzing flight in real time for possible hazardous situations.

LATAS enables users to create flight plans and to restrict their drones from flying outside of the intended area, thereby reducing the risk of capturing data that the user may not have permission to capture. The platform also allows operators to validate their actual flight against the flight plan they created – this feature serves as a secondary check to ensure that only the intended data, and not any unwanted data, has been collected. After the validation stage, if the user identifies any unwanted data, such data can be easily deleted through the platform's functionality. This system makes it possible to collect more precise and useful data.

[12] The LATAS (Low Altitude Traffic and Airspace Safety) platform connects leading airspace management technologies, such as sense and avoid, geo-fencing and aircraft tracking, into a service package for commercial and recreational drone operators as well as regulators and air traffic controllers. *See* http://flylatas.com.

Other systems provide similar functionality, allowing operators to establish geo-fences and providing pre-defined geo-fences around airports, critical infrastructure sites, and known dangerous areas. Operators using drones manufactured by 3DR can set custom geo-fencing before taking of or while flying, helping ensure that the drone will not fly over unauthorized areas or private property of others. [13] The U.S. Department of Interior has partnered with leading drone companies to provide operators with real-time geo-fencing data regarding firefighting activities on federal lands.[14] DJI, Airmap and Skyward are providing users with critical, timely notifications about wildfire areas that pilots should avoid; in the future, these geo-fencing systems will support real-time restrictions on operators' ability to fly into restricted airspace.[15]

Bureau of Land Management

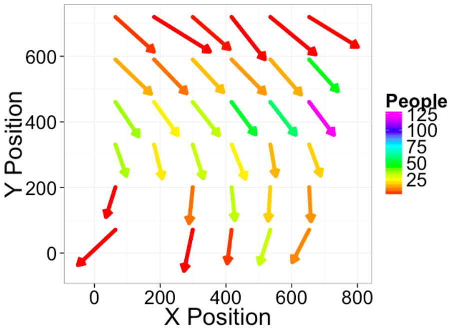
4. Embedding Privacy in the Design of Video Analytics

Information and imagery captured through drones might be processed using analytics software for numerous purposes, including statistics, research, or marketing. When the data collection is intended to count people who pass through a location or identify individuals' gender or age, but does not require identification of individuals, leading companies employ anonymous video analytic software (AVA), which relies on face detection and pattern recognition techniques. Using these technologies, person counts can be extracted and stored as a numerical log file, and the images or video can be discarded.

[13] Sollenberg, Roger. "Announcing The NAB Solo Software Release: The Biggest Software Update for A Drone – EVER." (blog), June 17, 2016. https://medium.com/3d-robotics/announcing-the-nab-solo-software-release-the-biggest-software-update-for-a-drone-ever-b02ccd5cd6d0#.w8njfpke0.

[14] "DJI and AirMap Deliver Real-Time Wildfire Awareness and Geofencing Capabilities for Drones." DJI NEWS. July 14, 2016. http://www.dji.com/newsroom/news/dji-and-airmap-deliver-real-time-wildfire-awareness-and-geofencing-capabilities-for-drones.

[15] "As Wildfire Season Continues to Heat Up, Dept. of Interior Partners with Industry to Eliminate Drone Intrusions." ENews Park Forest. July 25, 2016. http://enewspf.com/2016/07/25/wildfire-season-continues-heat-dept-interior-partners-industry-eliminate-drone-intrusions/.



4Quant Crowd Movement Trends

Various techniques exist for monitoring the movement of crowds while avoiding the collection of identifying images or mobile device data.[16] Researchers use these techniques to obfuscate personal data even when operators employ drone-mounted cameras to generate a constant stream of video information – data that would typically include identifiable images of particular individuals. By pairing streaming video output with image layering tools, live video feeds from multiple sources can be processed in real time while discarding the identifying image information. Then the data is then processed and analyzed in order to extract the information required, resulting in data plots that track numbers over time without identifying any of the individuals.

4Quant Real-Time In-Memory Analysis

Conclusion

As discussed above, leading drone companies are building privacy safeguards into their technologies and services. This report highlights technologies and practices that help drone operators minimize collection and retention of personal data, obfuscate images of individuals collected from the air, and secure personally identifiable information.

Companies are embedding privacy by design in sense and avoid solutions, building in security by design, embedding privacy in navigation controls, and employing anonymous video analytics that safeguard privacy. The widespread adoption of these

[16] E.g. "People Video Analytics." 4Quant.com. July 24, 2015. Accessed August 1, 2016. http://4quant.com/Drone-People-Counting/#learn-more; Calistra, Cole. "Anonymous Video Analytics (AVA) Technology & Privacy." Kairos. March 26, 2015. Accessed August 01, 2016. https://www.kairos.com/blog/155-anonymous-video-analytics-ava-technology-privacy.

technologies is enabling drones to reduce privacy risks while they tackle important, often life-saving missions.