

Potential Harms Associated with UAS

September 24, 2015

Introduction

This document identifies the risk of potential harms associated with the use of drones that may result from a lack of privacy, transparency, and accountability. The intent of this document is to open a discussion about risks and harms for unmanned aircraft systems (UAS), commonly referred to as drones.

Harms Associated With Lack of Privacy:

Harassment/Stalking

The use of a UAS involving unwanted, disturbing and threatening behavior toward a person, including following that person.

- A person or vehicle is manually or automatically tracked by a drone, causing them distress. (Think a drone-version of Gawker Stalker).

Invasion of Privacy

The use of a UAS to intrude on the private affairs of another person and/or disclosing that private information.

- Photographs of a person and her private living space are captured by a drone through a window without her consent. The photograph is posted online without the person's consent, and it is seen by others.
- A man is caught on camera leaving a strip club by a drone. The operator uploads the video online without his consent, causing him embarrassment.

Data Protection

The use of a UAS to collect information and unfairly use it without notifying the subject.

- A person finds her image being used on an advertisement after a drone takes the picture without her knowledge.

Trespass

The use of a UAS to intrude on another person's private property.

- A woman's property rights are violated when a drone is flying around her private airspace, such as her yard, without her permission.

Persistent Surveillance

The use of a UAS to linger on demand in an area to detect, locate, characterize, identify, track, or target people in near or real-time.

- A person has his movements throughout a city monitored by a drone over an extended period of time, revealing details about his personal life that he would prefer to keep private, such as his usual routes from church to home.
- A private drone constantly monitors a public park and posts all the footage online. The users of that public park would prefer the drone to stop filming so they can relax without their every move recorded for posterity and public comment.

Potential Harms Associated with UAS

September 24, 2015

Eavesdropping

The use of a UAS to listen to another person's private conversation with others.

- A couple has their private conversation recorded by a UAS with a long range directional microphone without the couple's consent.

Signals Collection

The use of a UAS to gather electronic transmissions.

- A teenager in a house with unsecure WiFi signals has his online search history collected by a drone that is flying overhead.
- A drone emulates a cell tower and picks up the phone numbers or MAC addresses of personal devices within range without consent of the device owners.

Harm from Identification

The forced identification of someone.

- A consumer using a drone delivery service to deliver products has his or her image and biometrics collected by a drone. That information is linked to online databases with more of the person's information. The person begins receiving unwanted advertising regarding that product.
- A hobbyist with a drone who wants to fly privately is forced to disclose when and where he will be flying his drone.
- A reporter investigating government corruption using her personal drone (e.g. to monitor police activity) is exposed after her drone's identifying markings reveal her identity.

Harms Associated with Lack Of Transparency:

Lack of Statement

The lack of a UAS privacy or transparency statement.

- A company that operates drones as part of its service does not have a transparency or privacy statement for those UAS. A consumer that uses the service is unable to identify what information was collected and how it is being used.

Deceptive Data Security and Privacy Practices

A business misleads their customers about their UAS policies.

- A consumer of a drone service is misled about what information is collected by that drone because its behavior contradicts the company's public policies and statements.
- A customer is misled about how information collected by a drone delivery service is shared with others because the company's public policies and statements are incorrect.

Identification

The inability to identify another's UAS.

- A drone that is flown over a public protest without any identifying marks chills speech because some protesters believe the drone to be law enforcement.

Potential Harms Associated with UAS

September 24, 2015

- Residents are upset when a drone flies through a residential neighborhood without identification because they are unable to find the drone operator and do not know the drone's purpose.

Harms Associated With Lack of Accountability:

Property Damage

The use of a UAS to damage another's property, whether accidentally or intentionally.

- A woman's car is damaged when a UAS falls and breaks a car windshield. A small business owner's property is damaged when a UAS crashes through a window of a building. The woman cannot identify the drone's owner and cannot seek recourse.
- A drone operator's device is damaged when another drone crashes into it. (Drone-on-drone violence). The owner cannot identify the drone's owner and cannot seek recourse.

Personal Injury

The use of a UAS to hurt another person, whether accidentally or intentionally.

- A boy is injured when a UAS crashes. The family cannot identify the drone's owner and cannot seek recourse.

Infrastructure Disruption

The use of a UAS to damage public infrastructure.

- A man's commute is disrupted when a drone crashes on a highway, creating a traffic jam. The operator cannot be identified.
- A neighborhood loses power when a drone crashes through a powerline. Authorities cannot identify the drone's owner. The operator cannot be identified.
- Homeowners and businesses are disrupted when a drone crashes and damages a local gas line. The operator cannot be identified.

Interference with First Responders

The use of a drone to disrupt law enforcement or first responders during an emergency.

- A firefighting helicopter is disrupted when an operator flies a drone over a wildfire. The drone is not identified.

Data Security & Privacy

The lack of data security for information collected by UAS.

- A consumer's information that was collected as part of a UAS service is exposed by hackers after the business fails to securely protect that information.

Harassment

The use of a UAS involving unwanted, disturbing and threatening behavior toward a person, including following that person.

- A person is persistently alarmed, annoyed, or tracked by a drone. For example, a user flew a drone on a public beach alarmingly close to people, hovering for minutes at a time, and taking pictures of them. Another example: A drone follows a person for a

Potential Harms Associated with UAS

September 24, 2015

period of time as she goes about her daily routine, though the person wishes the drone would cease following her.

Nuisance

The use of a UAS to annoy or bother another person.

- A family is bothered by a loud drone (maybe it just buzzes loudly, maybe it's playing music or honking its drone horn) that passes by and wakes them up early every morning.
- A person is upset when a drone that is surveying the neighboring building inadvertently captures their home as part of real-estate photography service.

Accountability Mechanism

The lack of an internal mechanism to deal with complaints from a UAS service.

- A consumer of a drone service complains to a business, but that business does not resolve the problem to the satisfaction of the consumer.
- An individual wants to register a concern with a UAS operator, but the operator does not provide any publicly accessible means of submitting a complaint or comment.
- A company creates a UAS privacy policy, but fails to adequately review compliance of that policy.

Corporate Intelligence Gathering

The use of a UAS to steal trade secrets such as by the removal, copying or recording of confidential or valuable information in a company for use by a competitor.

- A business has its intellectual property or other sensitive business information gathered by a drone.

Use Cases Subgroup: Harley Geiger, Mark Bathrick, Stephanie Spear, Liz Woolery, Carl Szabo, and Alan McQuinn Szabo, and Alan McQuinn

For Further Contact: Alan McQuinn, ITIF, (202) 524 – 5549, amcquinn@itif.org