

Chapter 25

Drones and Privacy

Nigel McKelvey

Letterkenny Institute of Technology, Ireland

Cathal Diver

Letterkenny Institute of Technology, Ireland

Kevin Curran

Ulster University, UK

ABSTRACT

Drones, also referred to as UAV's (Unmanned Aerial Vehicle), are an aircraft without a human pilot. Drones have been used by various military organisations for over a decade, but in recent years drones have been emerging more and more in commercial and recreational capacity. The paper is aimed at drone and UAV technology capabilities and how they could and are currently effecting privacy laws globally in comparison to those currently in the Rep. of Ireland. Being investigated is the collection, retention and purpose of which civilian's information is being gathered. The authors also discuss the laws preventing the development and evolution of drone technology in the US in comparison to the Rep. of Ireland.

1. INTRODUCTION

In today's society the monitoring of flights has never been more regulated, and it would be difficult to argue the reasons why because in 2013 global terrorism rose by 43% alone (Ackerman, 2014). With terrorism on the rise and the use of drones in society, drones could become prime targets for terrorists and criminals, not necessarily to use the devices to crash into densely populated areas, injuring and potentially killing people, but to harvest the information on the drones to aid criminals and terrorists in cyber/digital crimes that could range from theft of personal bank details to the loss of highly sensitive military recon footage. With the FAA in the U.S. reporting that by 2020 there could be as many as 30,000 drones in the sky in the U.S. alone, concerns about privacy, security and safety could be justified (Waterman, 2012). If these projections are to be believed and drones are set to become a part of our everyday society then laws must be ratified for the use and policing of these machines specifically in civilian zones where human safety must be paramount.

DOI: 10.4018/978-1-5225-8365-3.ch025

Figure 1. Phantom advanced and pro-650-80 (TechRadar, 2015)



Companies like Google and Facebook started acquiring drone companies such as Titan Aerospace, an American based drone maker which specializes in high altitude long endurance flights, and Ascenta, a British based drone maker that also specializes in high altitude long endurance flights, in 2014 respectively, acquiring them in order to research develop drones that could potentially stay in the air for years without landing. These giants of the tech world are essentially internet companies, entirely dependent on we the consumer having access to the internet, which is the answer to the question. The more people they have using their systems, the more money they generate, as of the 2nd financial quarter in 2014 90% of Google's generated revenue came from Google websites or Google Member websites (investor.google.com, 2014), these companies are exploring the possibility of using these aforementioned drone companies to provide internet to regions in the world that currently have little to no access to the web. This could potentially be a great service even if it is just to increase profits for their companies, but the protection and confidentiality of customer information must be a priority for these projects, with drones from Titan Aerospace potentially having flight times as long as 5 years then user information privacy and security must take priority over even performance (Winter, 2014).

The track record of drones being hacked doesn't inspire confidence with Professor Todd Humphreys and his colleagues at the Radio Navigation Lab at the University of Texas demonstrated to the U.S. Department of Homeland Security how they could hack a drone, owned by the University, using a "spoofing" technique making the drone mistake their commands for those of the GPS satellite. Todd Humphreys and his colleagues were working off a budget of \$1000, which is a nominal fee for something which could potentially cause catastrophic damage (BBC News, 2012). This same technique was used in late 2011 when a CIA guided recon drone had been hacked by enemy forces whilst flying over enemy territory in Iran. An engineer tasked with uncovering the drones stealth and security secrets claimed "The GPS navigation is the weakest point," when referring to the security of the drone (Peterson, 2011). The drone was hacked and landed by enemy forces with it containing very sensitive information. The DHS has since dismissed these accusations and claimed that it was a technical fault in the drone that forced it to crash land in enemy territory. If the accusations are true this would portray commercial drones in a bad light if state of the art military drones can be hacked so easily. Friday 26th of September 2014 is

13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/drones-and-privacy/226853

Related Content

Airplane Health Surveillance System: For Connected World

N. B. Rachana, K. G. Srinivasa and S. Seema (2016). *International Journal of Aviation Systems, Operations and Training* (pp. 11-24).

www.irma-international.org/article/airplane-health-surveillance-system/184761

Approach Operations and the Energy Management Challenge

Kevin M. Smith (2016). *International Journal of Aviation Systems, Operations and Training* (pp. 1-10).

www.irma-international.org/article/approach-operations-and-the-energy-management-challenge/184760

Intelligent Modeling of Risk Factors Contributing to Runway Incursion

Antonia Replogle, John E. Bischoff, Christopher J. Willy and Robert A. Roncace (2014). *International Journal of Aviation Systems, Operations and Training* (pp. 23-34).

www.irma-international.org/article/intelligent-modeling-of-risk-factors-contributing-to-runway-incursion/138607

The Synergy Between Tourism, Aviation, and Digital Transformation: A Path to Seamless Travel Experiences

Gonca Güzel ahin (2024). *Harnessing Digital Innovation for Air Transportation* (pp. 126-149).

www.irma-international.org/chapter/the-synergy-between-tourism-aviation-and-digital-transformation/340958

Dynamic Modeling and Control Techniques for a Quadrotor

Heba Elkholy and Maki K. Habib (2019). *Unmanned Aerial Vehicles: Breakthroughs in Research and Practice* (pp. 20-66).

www.irma-international.org/chapter/dynamic-modeling-and-control-techniques-for-a-quadrotor/226824